普通高等教育“十一五”国家级规划教材

高等院校信息安全专业系列教材

教育部高等学校信息安全类专业教学指导委员会
中国计算机学会教育专业委员会
共同指导

顾问委员会主任：沈昌祥　编委会主任：肖国镇

# 网络安全防御技术实践教程

黄传河　喻涛　王昭顺　编著

Information Security

http://www.tup.com.cn

清华大学出版社

高等院校信息安全专业系列教材

# 网络安全防御技术实践教程

黄传河　喻　涛　王昭顺　编著

清华大学出版社

北　京

## 内 容 简 介

本书主要针对高等院校计算机科学与技术、通信工程、计算机网络等相关专业，在计算机网络基础理论、网络安全基础理论学习完成之后，配套使用的网络安全实验教程。本书介绍了在局域网组建过程中，使用的多项安全产品及相关技术，包括网络防火墙、IDS入侵检测系统、USG统一网关和综合网络安全实践教程。

本书分为4篇，按照局域网组建中使用到的网络安全产品，详细讲述了使用这些网络安全设备，解决实际生活中遇到的各种安全问题，包括网络防火墙应用技术、入侵检测系统应用技术、统一网关应用技术等，以及针对这些问题的解决方法。本书在每个章节中对所使用到的相关安全产品的基本配置、基本界面、功能配置都给予了详细的讲解，以帮助读者熟悉产品的使用，并进一步诠释其在工程项目中的实施方法。

本书可作为高等院校计算机科学与技术、通信工程、计算机网络等相关专业本科生或研究生学习和研究网络安全产品及技术的实验教材，还可作为网络安全专业认证的培训教材，以及网络设计师、网络工程师、系统集成工程师以及其他专业技术人员在工作中遇到网络安全问题时的技术参考用书。



**图书在版编目（CIP）数据**

网络安全防御技术实践教程/黄传河，喻涛，王昭顺编著．—北京：清华大学出版社，2010.1
（高等院校信息安全专业系列教材）
ISBN 978-7-302-20983-6

Ⅰ．网…　Ⅱ．①黄…　②喻…　③王…　Ⅲ．计算机网络—安全技术—高等学校—教材
Ⅳ．TP393.08

中国版本图书馆CIP数据核字（2009）第164619号

**责任编辑：** 谢　琛　赵晓宁
**责任校对：** 白　蕾
**责任印制：**

**出版发行：** 清华大学出版社　　**地　址：** 北京清华大学学研大厦A座
http://www.tup.com.cn　　**邮　编：** 100084
**社 总 机：** 010-62770175　　**邮　购：** 010-62786544
**投稿与读者服务：** 010-62776969，c-service@tup.tsinghua.edu.cn
**质 量 反 馈：** 010-62772015，zhiliang@tup.tsinghua.edu.cn
**印 刷 者：**
**装 订 者：**
**经　销：** 全国新华书店
**开　本：** 185×260　　**印　张：** 20.75　　**字　数：** 484千字
**版　次：** 2010年1月第1版　　**印　次：** 2010年1月第1次印刷
**印　数：** 1～0000
**定　价：** 0.00元

本书如存在文字不清、漏印、缺页、倒页、脱页等印装质量问题，请与清华大学出版社出版部联系调换。联系电话：010-62770177转3103　　产品编号：033445-01

高等院校信息安全专业系列教材

# 编审委员会

# 出版说明

21 世纪是信息时代，信息已成为社会发展的重要战略资源，社会的信息化已成为当今世界发展的潮流和核心，而信息安全在信息社会中将扮演极为重要的角色，它会直接关系到国家安全、企业经营和人们的日常生活。随着信息安全产业的快速发展，全球对信息安全人才的需求量不断增加，但我国目前信息安全人才极度匮乏，远远不能满足金融、商业、公安、军事和政府等部门的需求。要解决供需矛盾，必须加快信息安全人才的培养，以满足社会对信息安全人才的需求。为此，教育部继 2001 年批准在武汉大学开设信息安全本科专业之后，又批准了多所高等院校设立信息安全本科专业，而且许多高校和科研院所已设立了信息安全方向的具有硕士和博士学位授予权的学科点。

信息安全是计算机、通信、物理、数学等领域的交叉学科，对于这一新兴学科的培养模式和课程设置，各高校普遍缺乏经验，因此中国计算机学会教育专业委员会和清华大学出版社联合主办了“信息安全专业教育教学研讨会”等一系列研讨活动，并成立了“高等院校信息安全专业系列教材”编审委员会，由我国信息安全领域著名专家肖国镇教授担任编委会主任，共同指导“高等院校信息安全专业系列教材”的编写工作。编委会本着研究先行的指导原则，认真研讨国内外高等院校信息安全专业的教学体系和课程设置，进行了大量前瞻性的研究工作，而且这种研究工作将随着我国信息安全专业的发展不断深入。经过编委会全体委员及相关专家的推荐和审定，确定了本丛书首批教材的作者，这些作者既在本专业领域有深厚的学术造诣，又有在教学第一线有丰富的教学经验。

本系列教材是我国第一套专门针对信息安全专业的教材，其特点是：

① 体系完整、结构合理、内容先进。

② 适应面广：能够满足信息安全、计算机、通信工程等相关专业对信息安全领域课程的教材要求。

③ 立体配套：除主教材外，还配有多媒体电子教案、习题与实验指导等。

④ 版本更新及时，紧跟科学技术的新发展。

为了保证出版质量，我们坚持宁缺毋滥的原则，成熟一本，出版一本，并保持不断更新，力求将我国信息安全领域教育、科研的最新成果和成熟经验反映到教材中来。在全力做好本版教材，满足学生用书的基础上，还经由专家的推荐和审定，遴选了一批国外信息安全领域优秀的教材加入到本系列教

材中，以进一步满足大家对外版书的需求。热切期望广大教师和科研工作者加入我们的队伍，同时也欢迎广大读者对本系列教材提出宝贵意见，以便我们对本系列教材的组织、编写与出版工作不断改进，为我国信息安全专业的教材建设与人才培养做出更大的贡献。

“高等院校信息安全专业系列教材”已于2006年初正式列入普通高等教育“十一五”国家级教材规划（见教高[2006]9号文件《教育部关于印发普通高等教育“十一五”国家级教材规划选题的通知》）。我们会严把出版环节，保证规划教材的编校和印刷质量，按时完成出版任务。

2007年6月，教育部高等学校信息安全类专业教学指导委员会成立大会暨第一次会议在北京胜利召开。本次会议由教育部高等学校信息安全类专业教学指导委员会主任单位北京工业大学和北京电子科技学院主办，清华大学出版社协办。教育部高等学校信息安全类专业教学指导委员会的成立对我国信息安全专业的发展将起到重要的指导和推动作用。“高等院校信息安全专业系列教材”将在教育部高等学校信息安全类专业教学指导委员会的组织和指导下，进一步体现科学性、系统性和新颖性，及时反映教学改革和课程建设的新成果，并随着我国信息安全学科的发展不断修订和完善。

我们的 E-mail：zhangm@tup.tsinghua.edu.cn；联系人：张民。

清华大学出版社

# 前 言

随着 21 世纪的到来，人类步入信息社会，信息产业成为全球经济发展的主导产业，计算机科学与技术在信息产业中占据了重要的地位。随着互联网技术的普及和推广，网络技术更是信息社会发展的推动力，人们在日常学习、生活和工作中都越来越依赖于网络，因此关于信息技术、信息安全技术、网络安全技术的发展成为越来越重要的学科。

互联网技术的发展改变了人们的生活，信息安全的内涵已发生了根本变化。安全已从一般性的安全防卫，变成了一种非常普通的安全防范；从一种研究型的学科，变成了无处不在，影响人们学习、生活和工作的安全技术。技术的普及也推动了社会对人才的需求，因此建立一套完整的网络安全课程教学体系，提供体系化的安全专业人才培养计划，培养一批精通安全技术的专业人才队伍，对目前高校计算机网络安全方向专业人才培养来说，显得尤为重要。

## 1. 关于教材开发背景

结合国家十二五本科计算机专业课程规划体系，深入领会教育部计算机科学与技术教学指导委员会编制的“计算机科学与技术专业规范的知识体系和课程大纲”文件精神，为及时反映目前网络安全专业学科发展动态，创新网络教材编辑委员会组织编写了本书。希望本书中的网络安全知识内容，既重视理论、方法和标准的介绍，又兼顾技术、系统和应用分析，在内容结构和知识点布局上能有所创新。

此外，随着互联网技术的普及和推广，人们日常学习和工作依赖网络的比重增加，计算机网络安全的实施和防范技术，成为目前最为瞩目的学习内容。因此，创新网络教材编辑委员会选择网络安全技术在生活中的具体应用作为教材开发主线，规划出面向实际工程案例，可操作、可应用、可实施的网络安全技术教程。同时希望策划的安全技术直观、形象、具体、可实施，选编和策划的安全知识具有专业化、体系化、全面化特征，能体现和代表当前最新的网络安全技术发展方向。

## 2 关于教材开发指导思想

通过市场调查发现，目前市场上指导计算机网络安全实践教学内容的教材非常匮乏。翻阅市场上品种有限的网络安全类教材，都侧重于网络安全理论诠释，而针对实际网络安全工程实施、可在课堂中动手实践的安全类教材

很少。因此，创新网络教材编辑委员会邀请国内院校专家，组织来自一线的专业工程师，联合开发了这本覆盖网络安全技术专业教程的教材，希望着重培养学生对网络安全技术的动手实践能力。

和同类以网络安全技术为研究方向的专业书籍相比，本书更注重解决实际工作中遇到的安全问题的能力。全书以安全技术应用为主线，以培养学生安全问题解决能力为目标，以加强实际安全技能锻炼为根本，满足学校安全类课程实践教学的需求。因此，本书在开发过程中，强化了实践教学能力的培养，着重讲授生活中的网络安全问题，诠释相应的安全策略配置。最终依据学校提供的安全实践教学平台，直观、形象地诠释安全技术，帮助学生理解抽象的网络安全专业理论。

### 3. 关于教材开发内容

本书是针对高等院校计算机科学与技术、通信工程、网络工程等相关专业，在学习基础网络安全理论时，开发的配套网络安全实验教程。全书详细地介绍了组建局域网安全过程中，遇到的安全问题，使用了多项安全产品及其安全技术，包括网络防火墙、IDS 入侵检测系统、USG 统一网关和一个综合网络安全实践教程。全书在每个章节中对这些安全产品的基本配置、基本界面、功能配置都给予了详细的讲解，帮助读者深入了解网络安全项目的设计与实施。通过对本书全部内容的学习，读者更易牢固掌握安全技术，从而熟悉实施方案。

全书包括近 40 个难度不同的网络安全实验内容，适合学生循序渐进地学习。本书还可作为高等院校计算机科学与技术、通信工程、计算机网络等相关专业本科生或研究生计算机网络工程课程的实验教材。全书的实验设计和安排，以实际工程项目的需求为依据，旨在加深学生对网络安全工程所涉及的基础理论知识的透彻理解，从而提高学生网络安全工程相关的动手实践能力、分析问题和解决问题的能力。

### 4. 关于教材使用方法

通过全书提供的近 40 个安全技术实验的训练，帮助学生熟练掌握网络安全工程师所必备的基本实践技能。所有实验操作都以日常安全需求为主线串接知识，以问题解决过程作为核心。因此教师在使用本书时，可作为相关安全理论学习完成之后的实验补充，帮助学生加强对抽象安全理论的理解。也可以根据教学的实际情况，从中选择部分实验教学内容，要求学生在学完理论之后，完成适当数量和难度的实验以补充理论讲解知识的不足。由于书中全部内容都来自实际工程案例的总结，因此，本书可作为就业前实习用书，通过对一定数量的安全工程案例的学习，从而积累实际中遇到的安全施工经验，以增强安全类工程施工的能力和排除故障的能力。

### 5. 关于课程环境安排

本书覆盖计算机网络安全规划、组建和配置中涉及的主流网络安全设备配置管理技术，书中所有工程项目都来自于企业多年积累的工程案例。经过一线教师和企业工程师的提炼，按照再现企业工程项目的方式进行组织串接，每个工程项目都详细介绍了工程名称、工程背景、技术原理、工程设备、工程拓扑、工程规划、工作过程、结果验证等多个环节，循序渐进展现企业工程项目，并把这些工程项目在网络实验室中搭建出来。

为顺利实施本教程，每个课程学习者，除需要对网络技术有学习的热情之外，还需具备基本的计算机、网络、安全基础知识。这些基础知识提供了良好的脚手架，帮助读者理解本书中的网络技术原理，为网络技术的进阶提供良好帮助。为更好地实施这些安全实验内容，需要为本课程提供一个可实施交换、路由和安全技术的网络环境，从而再现这些网络工程项目，以方便本教材的有效实施。这种课程工作环境包括：一个可以容纳40人左右的网络实验室；不少于4组的工作台。每组工作台中包括组建基本网络的网络实验设备：二层交换机设备、三层交换机设备、模块化路由器设备、网络防火墙、入侵检测系统IDS、统一网关设备、测试计算机设备和若干根网络连接线（或制作工具）。

本书选择的工程项目来自厂商的案例，使用的网络实验设备也来自厂商，但本课程在策划中，力求全部的知识讲解和技术选择都具有通用性，以遵循行业内的通用技术标准。全书关于设备的功能描述、接口的标准、技术的诠释、协议的细节分析、命令语法的解释、命令的格式、操作规程、图标和拓扑图形的绘制方法都使用行业内的通用技术标准，以加强其通用性。

### 6. 关于课程时间安排

本书通过加强对学生网络安全设备的实践操作，积累企业一线网络安全工程实施经验，让学生可以深入地理解和掌握网络安全设备的配置和运行机制，了解网络安全项目发生的场景和实施过程。此外，借助网络安全实践教学平台，读者还可以学习网络安全设计、网络攻防和故障性能分析等相关知识。从而加强学生对网络安全技术的理解和掌握，以培养学生的动手实践和设计分析能力，培养新型人才。

本书可作为高等院校计算机科学与技术、通信工程、计算机网络等相关专业本科生或研究生学习和研究网络安全技术的实验教材。其前导性的课程包括计算机网络、局域网组建、路由和交换技术等基础性网络技术。本课程的课时在36～72学时，根据学校具体教学时间安排，读者可选择全部的内容作为实验对象，也可选择部分学习内容。课程时间安排一般在第三年学期段。学生在全面学习专业组网技术后，作为学生学完基础网络技术的提高和补充。此外还可以作为网络安全专业认证的培训教材，以及网络设计师、网络工程师、系统集成工程师以及其他专业技术人员在实际工作中遇到网络安全问题时的技术参考用书。

### 7. 关于课程资源

不同的网络专业课程教学都具有其本身的针对性，强化网络安全专业实践能力、强化安全技术应用和网络安全技能培养，是本课程区别于传统网络安全专业课程的特色之一。无论是前期为保证本课程的有效实施，在课程实施环境（网络实验室）上投入的资金，还是在课程规划思想上的创新，以及在本课程研发上投入的人力都具有优势。

为有效保证本课程在学校的实施，保证课程教学资源的长期提供——案例的及时提供、安全技术的更新、新技术的学习、课程学习中的技术交流和讨论等，本课程的研发队伍还专门投入人力和物力，为本课程建设专门的课程网络资源共享基地，以有效支持课程在实施的过程中，安全项目资源的更新，疑难问题的解决，课程实施方案的讨论等一系列服务工作，详细内容可以访问本课程实施相关网站：http://www.labclub.com.cn，可以获

得更多的资源支持。

### 8. 关于课程开发队伍

本书由创新网络教材编辑委员会组织院校教学一线的专家队伍，来自厂商的工程师联合编写而成。这些工作在各行业的专家，把自己多年来在各自领域中积累的网络安全技术教学和应用的工作经验，以及对网络安全技术的深刻理解融入本书中。

本书第一作者黄传河博士，是武汉大学计算机学院教授、博士生导师。黄传河博士主要研究方向为计算机网络（如移动互联网、移动 Ad Hoc 网络、无线传感器网络、无线 Mesh 网络、WDM 网络、网络互联），网络安全，分布并行处理，量子计算。其在计算机网络及网络安全领域多年具前瞻性的研究，为全书提供了技术方向引导，统编了教学应掌握的安全技术知识点，并为保证最终技术准确性承担了审阅工作。

本书第二作者喻涛工程师，是武汉大学计算机学院博士，星网锐捷网络有限公司高级工程师。喻涛博士曾先后在中国电信、中国网通和锐捷网络工作，有多年在网络一线从事售前工程师的工作背景，参与过多个运营商网络工程规划、施工和企业网整网安全的规划、实施工作，具有丰富的实际网络技术应用能力，故障排除解决和整网安全防范实施能力。其多年在网络一线的工作背景，参与过多个网络工程整网安全的规划、实施的经历，对全书再现企业的实际安全工程需求，安全技术的选择和应用，按照企业工作过程实施流程等都起到重要作用，他还承担了全书的资料整理和编撰工作。

王昭顺教授，博士生导师，北京科技大学计算机系主任。王昭顺博士主要从事信息安全技术，ASIC 芯片设计，软件技术研究；承担“863”，“973”，“国家自然科学基金”多项项目。其多年从事网络安全、信息安全研究员的经历，为全书技术细节的解释，安全技术准确性的描述起到重要把关作用。

此外，在本书的编写过程中，还得到了其他一线教师，技术工程师，产品经理安淑梅、汪双顶、李文宇、方洋、张选波、高峡、杨靖、张勇、蔡韡等的大力支持。他们积累的多年的来自教学和工程一线的工作经验，都为本书的真实性、专业性以及方便在学校教学、方便实施给予了有力的支持。

本书策划、编辑的过程历经近三年的时间，前后经过多次的修订，得到了很多同仁的大力支持，由于编写水平有限，错漏之处在所难免，敬请广大读者指正（labserv@ruijie.com.cn）。

创新网络教材编辑委员会

# 使用说明

为帮助学生全面理解安全技术细节，建立直观的网络安全印象，本书每个实验在开始时都为读者引入一个来自企业的真实网络安全问题，从而营造教学、学习环境，让读者深入到网络安全的场景环境中，以了解本书安全知识内容发生在真实网络工程项目中实际的场景，了解相应的在施工中需要的技术。

在全书关键技术解释和工程方案实施中，会涉及一些网络专业术语和词汇。为方便大家今后在工作中的实际应用，全书采用行业标准的技术和图形绘制方案。全书中使用的相关符号、网络拓扑图形惯有的风格和惯例，以及本书使用的命令语法规范约定如下：

- 竖线“|”表示分隔符，用于分开可选择的选项。
- 星号“*”表示可以同时选择多个选项。
- 方括号“[ ]”表示可选项。
- 大括号“{ }”表示必选项。
- **粗体字**表示按照显示的文字输入的命令和关键字。在配置的示例和输出中，粗体字表示需要用户手工输入的命令（例如 **show** 命令）。
- *斜体字*表示需要用户输入的具体值。

以下为本书中所使用的图标示例。






感谢网络产品和方案提供商星网锐捷网络有限公司，为全书提供多个、来自不同行业的工程案例。为方便对工程项目技术细节的诠释，本书技术描述主要围绕锐捷网络RGNOS网络操作系统展开。但在书中出现的所有命令和术语，同样具有通用性，能兼容目前网络工程施工中涉及的所有主流设备。本书中讲述的技术原理，以及针对网络问题提出的解决方案，同样适用于现实网络工作场景。

# 目 录

## 第 1 篇　防火墙安全



## 第 2 篇　入侵检测技术安全




# 防火墙安全

# 第 1 章 防火墙设备基础知识

## 1.1 什么是防火墙

防火墙的本义是指古代构筑木制结构房屋时，为了防止火灾的发生和蔓延，人们将坚固的石块堆砌在房屋周围作为屏障，这种防护构筑物就被称为"防火墙"。这道墙可以防止火灾发生时蔓延到别的房屋。当火灾发生时，这种防护构筑物对房屋中的人起到保护作用。

今天网络中通常所说的网络防火墙，是借鉴了古代防火墙的喻义，它指的是隔离在本地网络与外界网络之间的一道防御系统，是对所有实施网络安全防范措施的总称。防火墙英文名称为 FireWall，设置在不同网络之间，如可信任的企业内网和不可信的公共网(Internet)之间，或位于计算机和它所连接的网络之间的硬件或软件的组合，如图 1-1 所示。防火墙可以使企业内部局域网(LAN)与 Internet 之间或者与其他外部网络互相隔离、限制网络互访以保护内部网络。

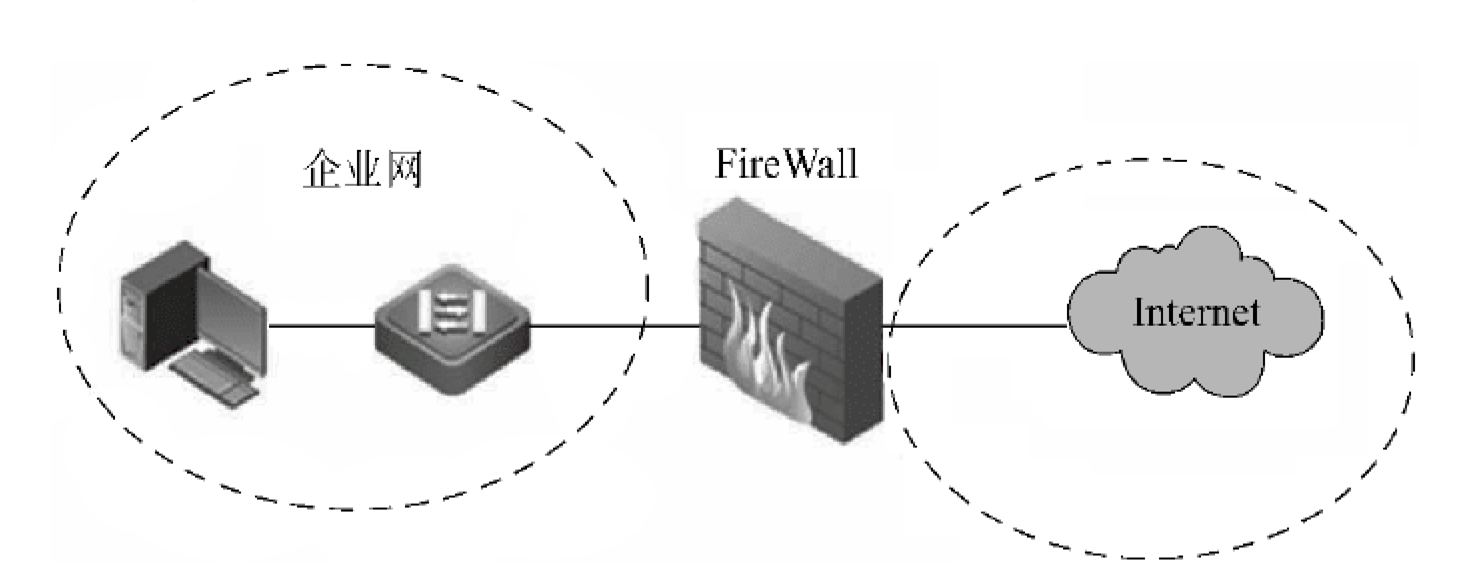



图 1-1　设置在内网和 Internet 间的防火墙

在互联网上防火墙是一种非常有效的网络安全模型，通过它可以隔离风险区域(即 Internet 或有一定风险的网络)与安全区域(局域网)的连接，同时不会妨碍人们对风险区域的访问。防火墙可以监控进出网络的通信量，从而完成看似不可能完成的任务；只让安全的信息进入，抵制了对企业构成威胁的数据。

防火墙多见于两个或多个网络之间，是不同网络间信息的唯一出入口。网络间所有数据流都要经过防火墙，由防火墙提供网络间的信息安全服务，防火墙根据企业网的安全政策，控制、允许、拒绝、监测出入网络间的信息流，提供安全防范保护功能，而且防火墙本身也具有较强的抗攻击能力。

一般的防火墙都可以达到以下目的：一是可以限制他人进入内部网络，过滤不安全服务和非法用户；二是防止入侵者接近防御设施；三是限定用户访问特殊站点；四是为监视 Internet 安全提供方便。由于防火墙假设了网络边界和服务，因此更适合于相对独立

的网络。例如,Intranet 等种类相对集中的网络。防火墙正在成为控制对网络系统访问非常流行的方法。事实上,在 Internet 上的 Web 网站中,超过 1/3 的 Web 网站都是由某种形式的防火墙来加以保护的,这是对黑客防范最严、安全性较强的一种方式,建议任何关键性的服务器都放在防火墙之后。

防火墙可以监控进出网络的通信量,从而完成看似不可能完成的任务:仅让安全通过验证的信息进入,同时又抵制对企业网络构成威胁的数据。随着网络上安全性问题的失误和缺陷越来越普遍,对网络的入侵不仅来自高超的攻击手段,也有可能来自配置上的低级错误或选择了不合适的口令。因此,防火墙的作用是防止恶意的、未授权的通信进出被保护的网络,迫使企业强化自己的网络安全政策。

## 1.2 防火墙的功能

在逻辑上,防火墙是一个分离器,一个限制器,也是一个分析器,有效地监控了内部网和 Internet 之间,或者内部网络之间的任何活动。防火墙可以对网络之间的通信进行扫描,关闭不安全的端口,阻止外来的 DoS 攻击,封锁木马的传播路径等,以保证网络安全。

典型意义上的防火墙设备具有三个方面的基本特性:内部网络和外部网络之间的所有数据流都必须经过防火墙;只有符合安全策略的数据流才能通过防火墙;防火墙自身具有非常强的抗攻击免疫力。

- 内部网络和外部网络之间的所有网络数据流都必须经过防火墙。

这是防火墙所处网络位置的特性,同时也是一个前提。因为只有当防火墙是内、外部网络之间通信的唯一通道,才可以全面、有效地保护企业网络不受侵害。

根据美国国家安全局制定的《信息保障技术框架》,防火墙适用于用户网络系统的边界,属于用户网络边界的安全保护设备。所谓网络边界即是采用不同安全策略的两个网络连接处,例如用户网络和互联网之间连接、和其他业务往来单位的网络连接、用户内部网络不同部门之间的连接等。防火墙的目的就是在网络连接之间建立一个安全控制点,通过允许、拒绝或重新定向经过防火墙的数据流,实现对进、出内部网络的服务和访问的审计和控制。

典型的防火墙体系网络结构如图 1-2 所示。从图 1-2 中可以看出,防火墙的一端连接企事业单位内部的局域网,而另一端则连接互联网。所有的内、外部网络之间的通信都要经过防火墙。

- 只有符合安全策略的数据流才能通过防火墙。

防火墙最基本的功能是确保网络流量的合法性,并在此前提下将网络的流量快速地从一条链路转发到另外的链路上去。从最早的防火墙模型开始谈起,原始的防火墙是一台"双穴主机",即具备两个网络接口,同时拥有两个网络层地址。防火墙将网络上的流量通过相应的网络接口接收上来,按照 OSI 协议栈的七层结构顺序上传,在适当的协议层进行访问规则和安全审查,然后将符合通过条件的报文从相应的网络接口送出,而对于那些不符合通过条件的报文则予以阻断。

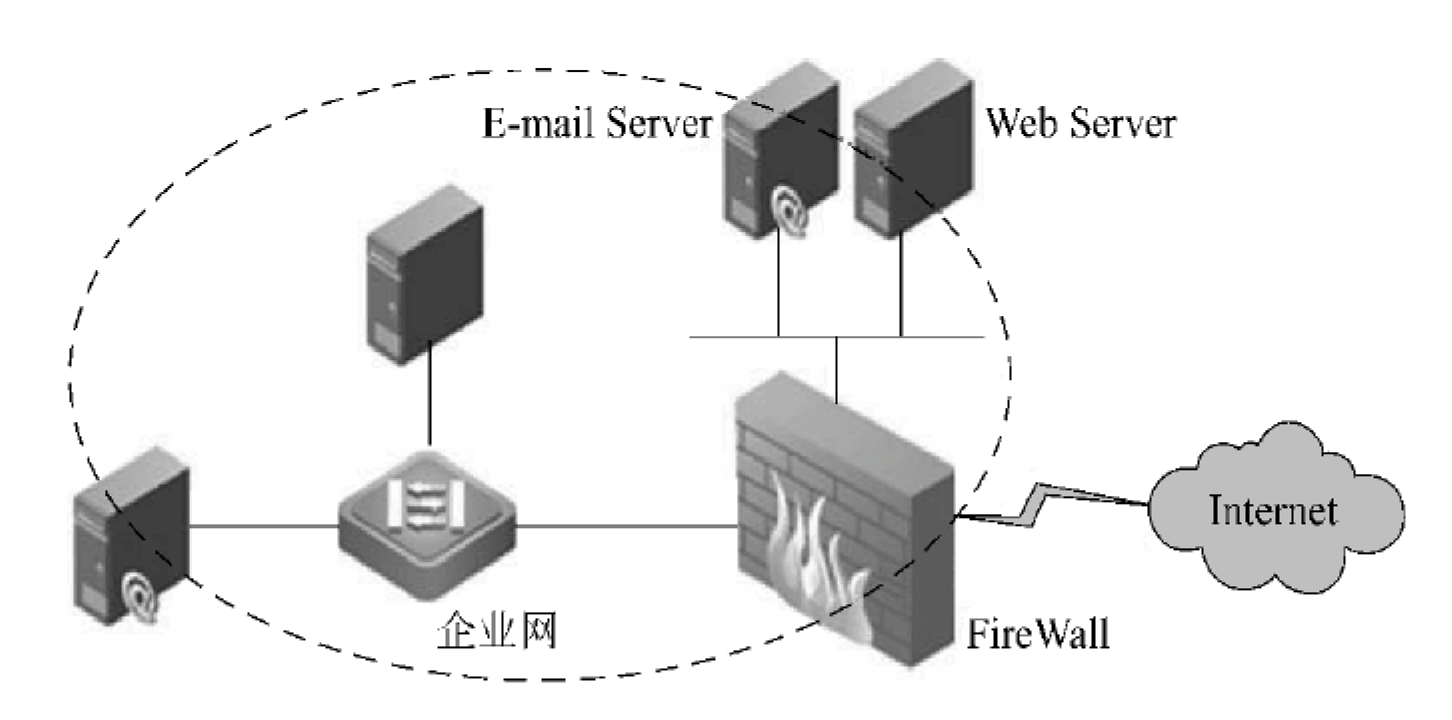



图 1-2　设置在企业网和 Internet 间的防火墙

因此，从这个角度上来说，防火墙是一个类似于桥接或路由器的、多端口的（网络接口≥2）转发设备，它跨接于多个分离的物理网段之间，并在报文转发过程中完成对报文的审查工作，如图 1-3 所示。

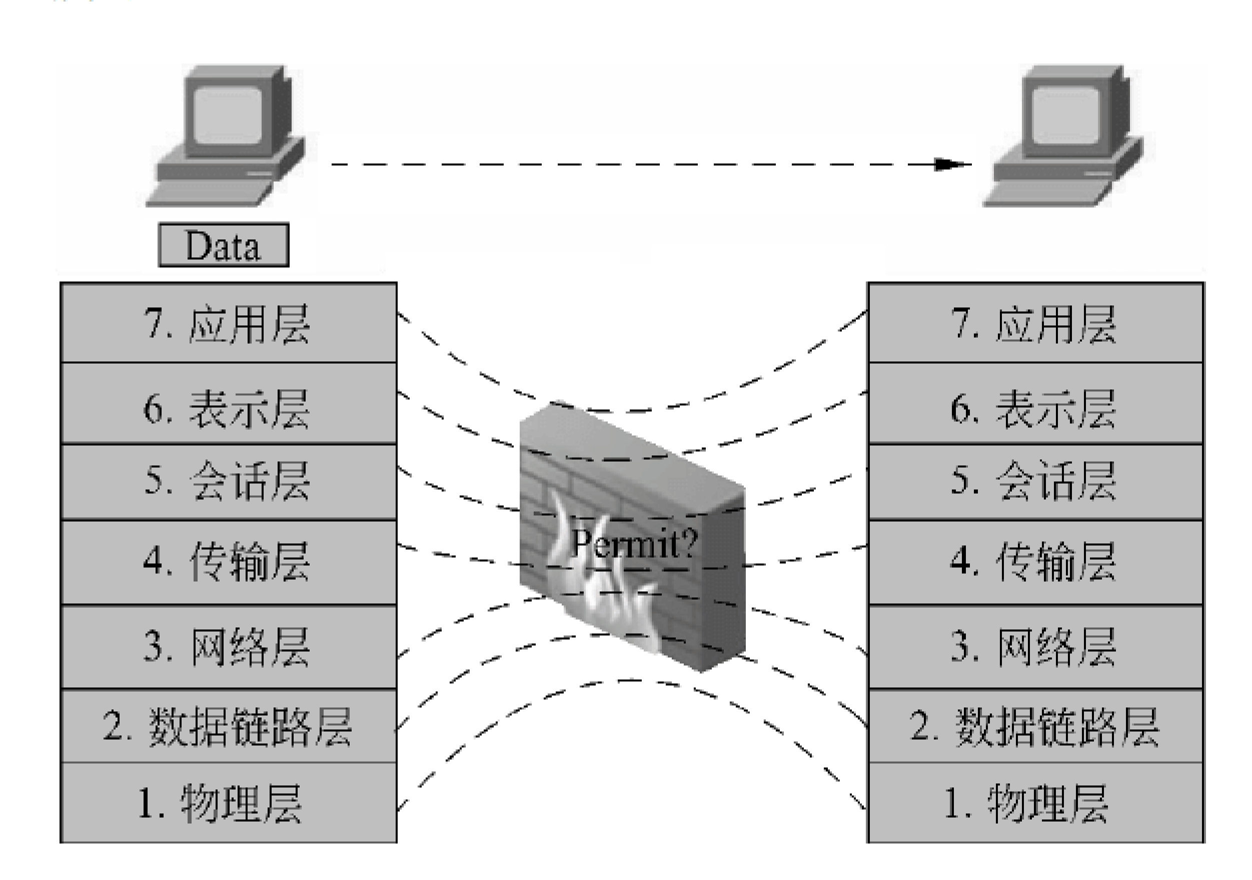



图 1-3　防火墙完成对报文的审查

- 防火墙自身应具有非常强的抗攻击免疫力。

这是防火墙之所以能担当企业内部网络安全防护重任的先决条件。防火墙处于网络边缘，它就像一个边界卫士，每时每刻都要面对黑客的入侵，这样就要求防火墙自身具有非常强的抗击入侵本领。之所以具有这么强的本领，防火墙操作系统本身是关键，只有自身具有完整信任关系的操作系统才可以谈论系统的安全性。其次就是防火墙自身具有非常低的服务功能，除了专门的防火墙嵌入系统外，再没有其他应用。

所有进出的信息都必须通过防火墙的验证，防火墙便成为安全问题的检查点，可疑的访问被拒绝于门外。但防火墙在防范网络时也具有很多不足的地方，防火墙的缺点主要表现在以下几个方面。

（1）不能防范恶意的知情者。

防火墙可以禁止系统用户经过网络连接发送专有的信息，但用户可以将数据复制到磁盘、磁带上，放在公文包中带出去。如果入侵者已经在防火墙内部，防火墙是无能为力的。内部用户可以偷窃数据，破坏硬件和软件，并且巧妙地修改程序而不接近防火墙。对于来自知情者的威胁，只能加强内部管理，如主机安全和用户教育等。

(2) 不能防范不通过它的连接。

防火墙能够有效地防止通过它的传输信息,然而却不能防止不通过它而传输的信息。例如,如果站点允许对防火墙后面的内部系统进行拨号访问,那么防火墙绝对没有办法阻止入侵者进行拨号入侵。

(3) 不能防备全部的威胁。

防火墙被用来防备已知的威胁,如果是一个很好的防火墙设计方案,就可以防备新的威胁,但没有一扇防火墙能自动防御所有新的威胁。

(4) 防火墙不能防范病毒。

防火墙一般不能消除网络上的病毒。

## 1.3 防火墙的工作原理

防火墙实际上就是网络上的一种过滤塞,可以让安全的信息流通过这个塞子,不安全的信息都统统过滤掉。所有的防火墙至少都会说两个词:Yes 或者 No,也就是接受或者拒绝。防火墙采用的技术和标准可谓五花八门,但最简单的防火墙模型类似于以太网桥设备,但几乎没有人会认为这种原始防火墙能起多大作用。

今天防火墙的形式多种多样:有的系统上已经装备了 TCP/IP 协议栈;有的在已有的协议栈上建立了自己的软件模块。还有一些应用型的防火墙只对特定类型的网络连接提供保护(比如 SMTP 或者 HTTP 协议等),还有一些基于硬件的防火墙产品,在日常网络的应用中,把以上的产品都叫做防火墙。因为它们的工作方式都是一样的:分析出、入防火墙的数据包,决定放行还是阻止通过。

所有的防火墙都具有 IP 地址数据包过滤功能,这项任务只需要检查 IP 数据包头部特征信息,如根据其 IP 源地址和目标地址,即可作出放行/丢弃决定动作。包过滤是在 IP 层实现的,包过滤根据包的源 IP 地址、目的 IP 地址、源端口、目的端口及包传递方向等报头信息来判断是否允许包通过,过滤用户定义的内容,如 IP 地址,如图 1-4 所示。其工作原理是系统在网络层检查数据包,与应用层无关。包过滤防火墙的应用非常广泛,因

<table>
<tr><td>版本 (4)</td><td>头长度 (4)</td><td>TOS(8)</td><td colspan="2">总长度 (16)</td></tr>
<tr><td colspan="3">标识 (16)</td><td>标志 (3)</td><td>段偏移 (13)</td></tr>
<tr><td colspan="2">TTL(8)</td><td>协议 (8)</td><td colspan="2">校验和 (16)</td></tr>
<tr><td colspan="5">源 IP 地址 (32)</td></tr>
<tr><td colspan="5">目的 IP 地址 (32)</td></tr>
<tr><td colspan="5">选项 (0 or 32 if any)</td></tr>
<tr><td colspan="5">数据</td></tr>
</table>

图 1-4 IP 数据包头部特征信息

为 CPU 用来处理包过滤的时间可以忽略不计。而且这种防护措施对用户透明，合法用户在进出网络时，根本感觉不到它的存在，使用起来很方便。这样系统就具有很好的传输性能，且易扩展。

但是这种防火墙不太安全，因为包过滤系统对应用层信息无法解析，也就是说，它们不理解通信的内容，不能在用户级别上进行过滤，即不能识别不同的用户和防止地址的盗用。如果攻击者把自己主机的 IP 地址设成一个合法主机的 IP 地址，就可以很轻易地通过包过滤器，这样更容易被黑客攻破。基于这种工作机制，包过滤防火墙有以下缺陷。

(1) 通信信息：包过滤防火墙只能访问部分数据包的头信息。

(2) 通信和应用状态信息：包过滤防火墙是无状态的，所以它不可能保存来自于通信和应用的状态信息。

(3) 信息处理：包过滤防火墙处理信息的能力是有限的。

代理服务型防火墙在应用层上实现防火墙功能，弥补了包过滤防火墙的不足。它能提供部分与传输有关的状态，提供与应用相关的状态，解析部分传输的信息，此外还能处理和管理信息。

## 1.4 防火墙的分类

目前市场上的防火墙产品非常多，划分的标准也比较杂。主要分类如下：

- 从软、硬件形式上分为软件防火墙和硬件防火墙以及芯片级防火墙。
- 从防火墙技术上分为“包过滤型”和“应用代理型”两大类。
- 从防火墙结构上分为单一主机防火墙、路由器集成式防火墙和分布式防火墙 3 种。
- 按防火墙的应用部署位置分为边界防火墙、个人防火墙和混合防火墙 3 大类。
- 按防火墙性能分为百兆级防火墙和千兆级防火墙两类。

## 1.5 防火墙技术

传统的防火墙多是基于访问控制列表（ACL）规则的 IP 包过滤防火墙，一般安装在企业内网的入口处，所以也俗称“边界防火墙”。随着网络安全事件的不断升级，防火墙技术也得到了新的发展，出现了一些新的防火墙技术，如电路级网关技术、应用网关技术和动态包过滤技术。在实际运用中，这些技术差别非常大，有的工作在网络层，有的工作在传输层，还有的工作在应用层。

从技术发展角度来看，尽管防火墙技术经过几代的革新，出现了很多不同的品种，但是按照防火墙对内外网络数据的处理方法，大致可以将防火墙分为两大体系：包过滤防火墙和应用代理防火墙（应用层网关防火墙）。

### 1. 包过滤防火墙

包过滤(PacketFilter)防火墙是防火墙常见的类型,也称为分组过滤防火墙,作用在网络层和传输层。包过滤是在网络层中对数据包实施有选择的通过,其技术依据是网络中的包传输技术。在互联网这样的信息包交换网络上,所有往来的信息都被分割成许许多多一定长度的信息包,包中包括发送者的 IP 地址和接收者的 IP 地址。网络上的数据都是以“包”为单位进行传输,数据被分割成为一定大小的数据包,每一个数据包中都携带传输数据的特征信息:如数据的源地址、目标地址、TCP/UDP 源端口和目标端口等,如图 1-5 所示。

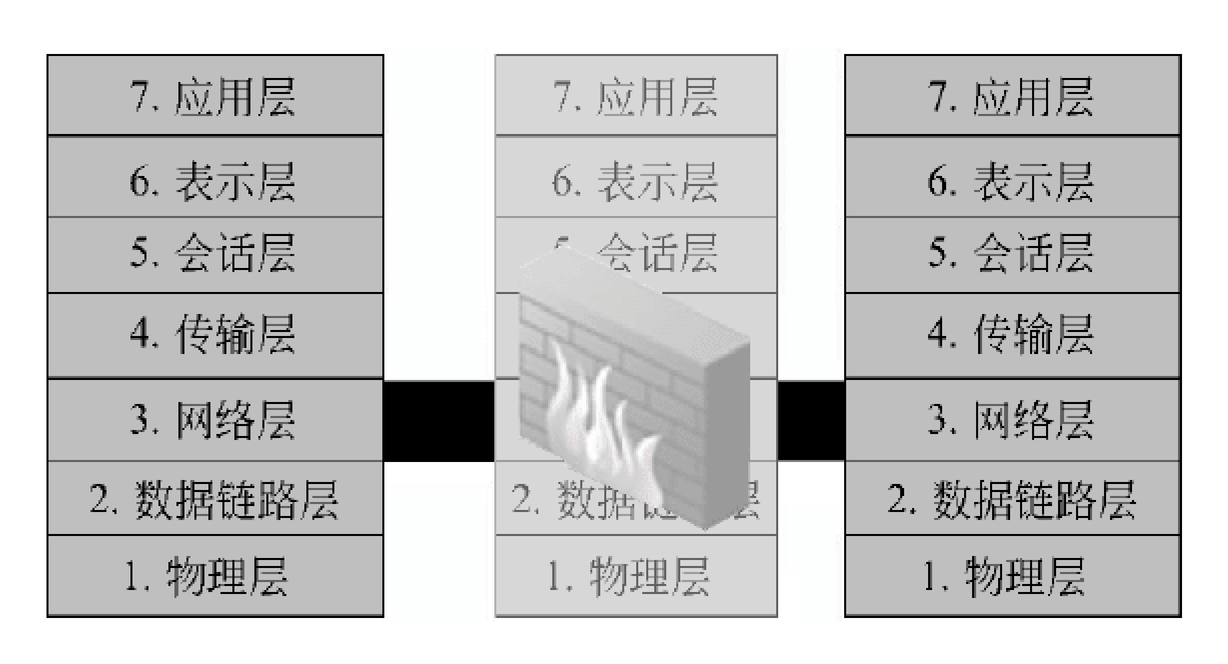



图 1-5 包过滤防火墙工作模型

包过滤防火墙判断所依据的信息,均来源于 IP、TCP 或 UDP 包头特征信息。通过读取数据包头中的特征信息,来判断这些“包”是否来自可信任的安全网络,从而确定是否允许数据包通过。防火墙依据系统事先设定好的过滤逻辑,检查数据流中的每个数据包,根据数据包的源地址、目标地址以及包所使用端口确定是否允许该类数据包通过。只有满足过滤规则的数据包,才会被防火墙转发到相应目标网络接口。一旦发现有来自危险网络的特征数据包,依据预先配置的过滤规则,防火墙便会将这些数据拒之门外。

包过滤防火墙会检查所有通过信息包中的 IP 地址,并按照系统管理员所给定的过滤规则过滤信息包。如果防火墙设定某一个 IP 为危险的话,从这个地址而来的所有信息都会被防火墙屏蔽掉。包过滤路由器的最大优点就是它对于用户来说是透明的,也就是说不需要用户名和密码来登录。这种防火墙速度快而且易于维护,通常作为第一道防线。

包过滤路由器的弊端也是很明显的,通常它没有用户的使用记录,这样就不能从访问记录中发现黑客的攻击记录。而攻击一个单纯的包过滤防火墙对黑客来说是比较容易的。此外,配置烦琐也是包过滤防火墙的一个缺点。它阻挡别人进入内部网络,但不告诉何人进入防火墙的系统,或者何人从内部进入网际网络。它可以阻止外部公有网络用户对私有网络的访问,却不能记录内部的访问。包过滤另一个关键的弱点就是不能在用户级别上进行过滤,即不能鉴别不同的用户和防止 IP 地址被盗用。包过滤型防火墙是某种意义上的相对安全的系统。

### 2 应用代理防火墙

应用代理防火墙也可以称为代理服务器，它的安全性要高于包过滤型产品。应用代理防火墙工作在应用层，其特点是能够完全阻隔网络中通信的数据流，通过对每种应用服务编制专门的代理程序，实现监视和控制应用层通信流的作用。应用代理防火墙一般安装在内部网与外部网的隔离点，起着监视和隔绝应用层通信流的作用。它通常工作在 OSI 模型的最高层，掌握着应用系统中安全决策的全部信息，如图 1-6 所示。

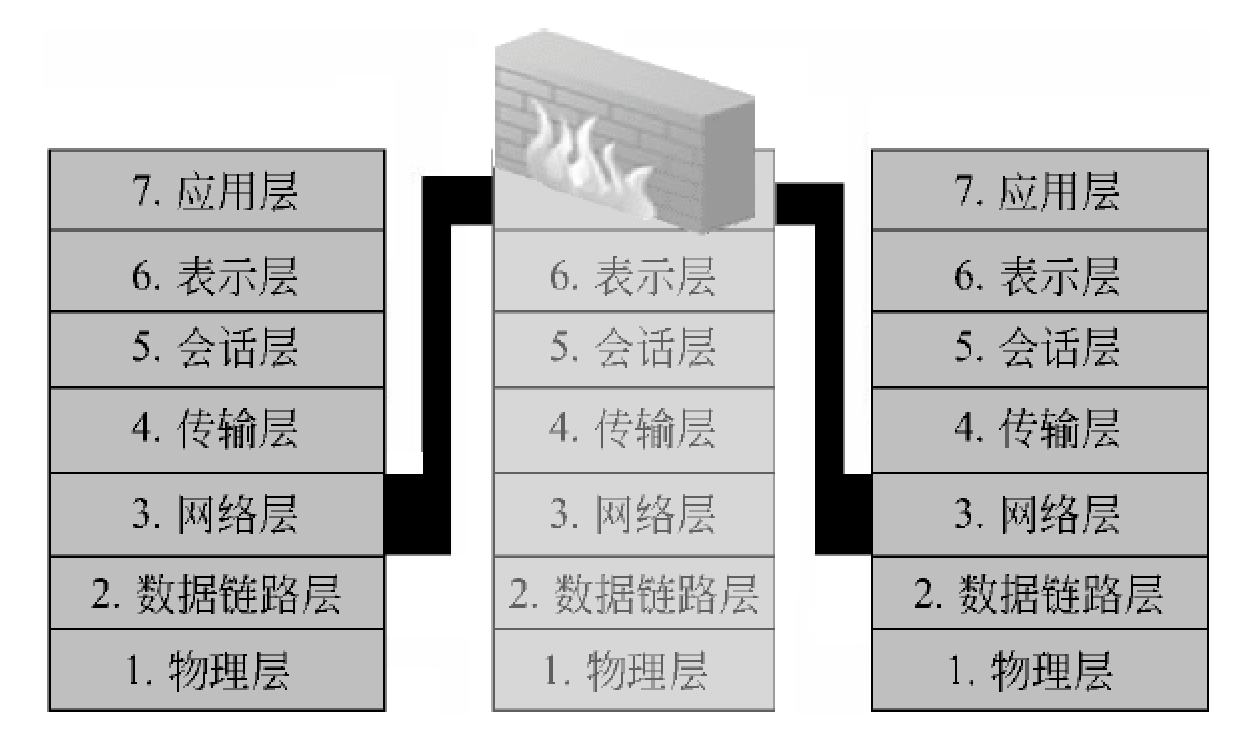



图 1-6　应用代理防火墙工作模型

应用代理服务器通常也称作应用级防火墙。包过滤防火墙是按照 IP 地址来禁止未授权者的访问，但是它不适合单位用来控制内部人员访问外界的网络，对于这样的企业来说应用级防火墙是更好的选择。所谓代理服务，即防火墙内外的计算机系统应用层的链接，是在两个终止于代理服务的链接实现的，这样便成功地实现了防火墙内外计算机系统的隔离。代理服务是设置在 Internet 防火墙网关上的应用，网络管理人员可以在其上设置特定的允许或拒绝服务。同时，还可应用于实施较强的数据流监控、过滤、记录和报告等功能。一般情况下可应用于特定的互联网服务，如超文本传输（HTTP）、远程文件传输（FTP）等。代理服务器通常拥有高速缓存，缓存中存有用户经常访问站点的内容，在下一个用户要访问同样的站点时，服务器就用不着重复地去抓同样的内容，既节约了时间也节约了网络资源。

## 1.6　硬件防火墙设备

从防火墙技术表现的形式上来分，防火墙大致分为硬件防火墙和软件防火墙两类。

软件防火墙其实就是安全防护软件，是运行于特定的计算机平台上的软件产品，它需要客户预先安装好的计算机操作系统的支持，一般来说这台计算机就是整个网络的网关，俗称“个人防火墙”。

一些操作系统包含了内置防火墙，如图 1-7 所示；而有些软件防火墙就像其他软件产品一样，需要先在计算机上安装并做好配置才可以使用，它通过在操作系统底层工作来实现网络管理和防御功能的优化。随着宽带网络的迅速发展，软件防火墙在大数据流量面前显得力不从心，例如诺顿防火墙、天网防火墙、金山网镖、瑞星防火墙等，系统防火墙如图 1-8 所示。




图 1-7　软件防火墙

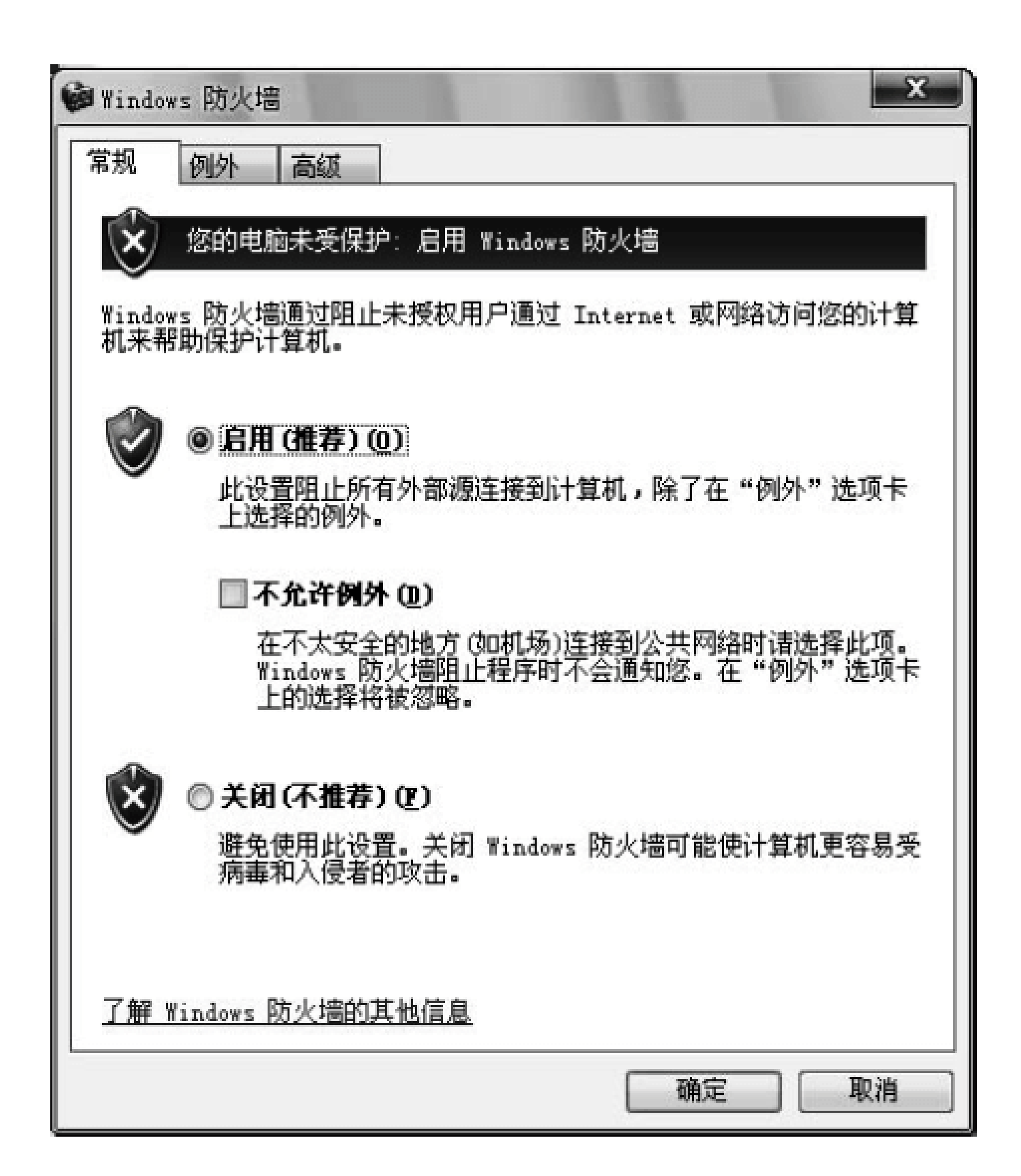



图 1-8　系统防火墙

硬件防火墙，通常也称为网络防火墙，基于硬件的防火墙应用于保护整个网络，这里所说的硬件防火墙是指具有独立芯片防火墙设备，具有专用的硬件平台。硬件防火墙是指把防火墙程序做到芯片里面，由硬件执行这些功能，以减少 CPU 的负担，使路由更稳定，如图 1-9 所示。硬件防火墙是保障内部网络安全的一道重要屏障。它的安全和稳定，直接关系到整个内部网络的安全。硬件防火墙一般有这样的核心要求：它的硬件和软件都需要单独设计，有专用网络芯片来处理数据包；同时，采用专门的操作系统平台，从而避免通用操作系统的安全方面的漏洞。




图 1-9　硬件防火墙

硬件防火墙一般都有 WAN、LAN 和 DMZ 3 种类型的端口，分别连接 3 种不同网络区域，具有不同级别的安全防范功能，如图 1-10 所示。硬件防火墙具有多种安全防范功能，价格比较高，企业以及大型网络使用得比较多。需要在硬件防火墙上设置适当的规则，利用这些规则防火墙对流经自己的数据作出判断，让这些数据通过或者不通过，以达到禁止非正常数据通过，保护网络安全的目的。通常硬件防火墙部署在网络的出口或者是网络重点保护区域，需要完成两个工作：第一，作为网络互联设备实现网络互联互通；第二，作为网络安全设备检测流经数据，以保护网络安全。

目前市场上大多数防火墙都是这种硬件防火墙，大多是基于 PC 架构，也就是说，它们的架构和普通的家庭用 PC 没有太大区别。在这些 PC 架构计算机上运行一些经过裁剪和简化的操作系统，最常用的有老版本的 UNIX、Linux 和 FreeBSD 系统。值得注意的

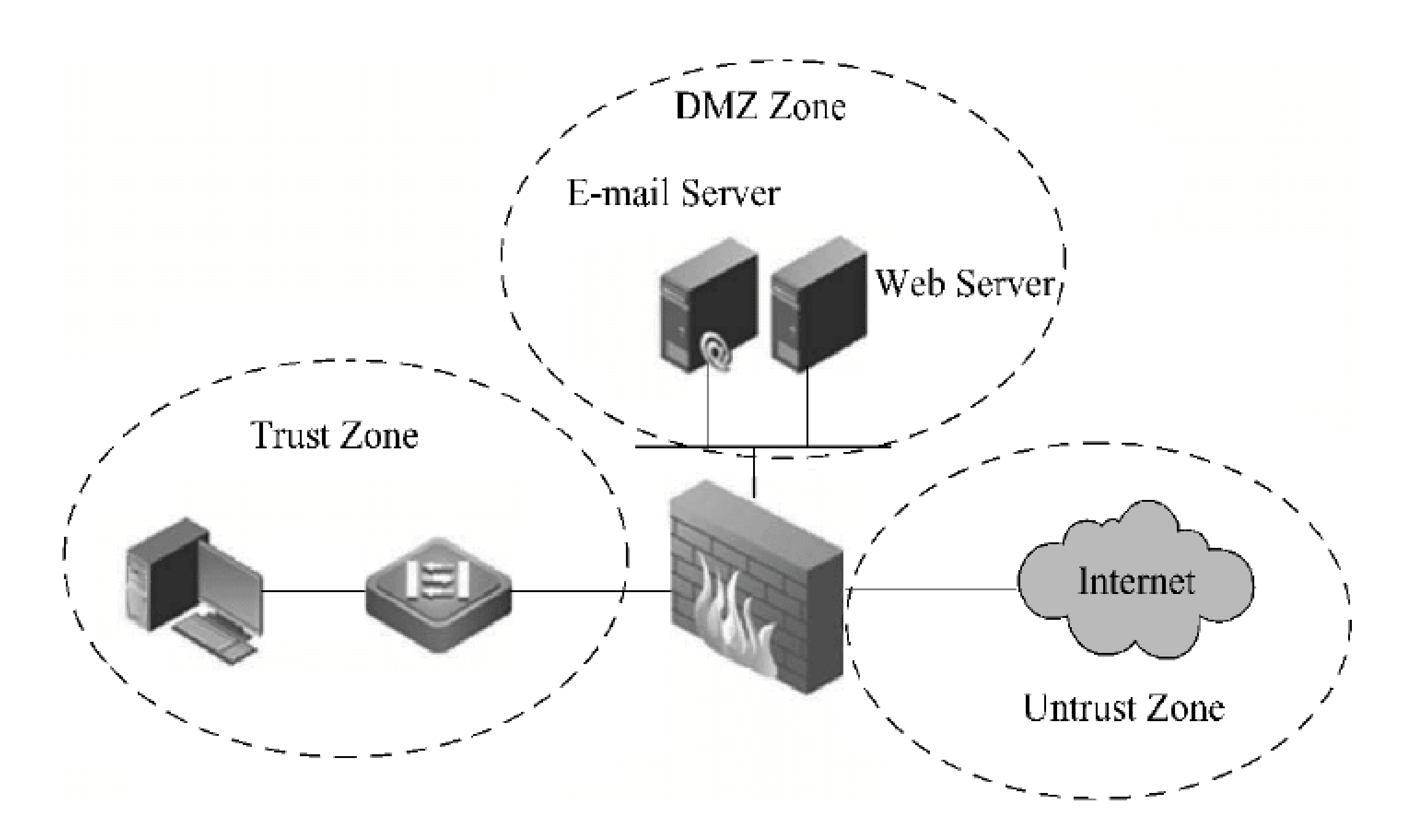



图 1-10　防火墙产品防范 3 个区域安全

是，由于此类防火墙采用的依然是 PC 的内核，因此依然会受到操作系统本身的安全性影响。

早期的千兆防火墙仅仅是将百兆接口替换为千兆接口而已。这种基于 PC 模式的 X86 体系结构的千兆防火墙主体仍然是软件，其性能受到很大制约，无法达到千兆的处理速度。因此，这些防火墙只是具有千兆接入能力的防火墙，而不是真正具有千兆处理能力。随着千兆网络在企业和行业用户中的不断普及，以及用户对性能需求的不断增加，千兆防火墙也逐渐发生了质变。

这种质的变化首先是人们把目光转移到了专用集成电路（ASIC）和网络处理器（NP）上。相对于 X86 架构，基于这些架构的千兆防火墙才是真正的硬件解决方案，能够实现千兆处理速度。

### 1. X86 架构

最初的千兆防火墙是基于 X86 架构的。X86 架构采用通用 CPU 和 PCI 总线接口，具有很高的灵活性和可扩展性，过去一直是防火墙开发主要平台。其产品功能主要由软件实现，可以根据用户的实际需要而做相应调整，增加或减少功能模块。产品比较灵活，功能十分丰富。

但其性能发展却受到 X86 体系结构的制约，作为通用的计算平台，X86 的结构层次较多，不易优化，且往往会受到 PCI 总线的带宽限制。虽然 PCI 总线接口理论上能达到接近 2Gb/s 的吞吐量，但是通用 CPU 的处理能力有限。尽管防火墙软件部分可以最大限度地优化，但很难达到千兆速率。同时很多 X86 架构的防火墙是基于定制的通用操作系统，其安全性很大程度上取决于通用操作系统自身的安全性，可能存在安全漏洞。

### 2. ASIC 架构

相比之下，ASIC 防火墙通过专门设计的 ASIC 芯片逻辑进行硬件加速处理。ASIC 架构防火墙通过把指令或计算逻辑固化到芯片中，获得了很高的处理能力，因而明显提升了防火墙的性能。新一代的高可编程 ASIC 架构采用了更灵活的设计，能够通过软件改变应用逻辑，具有更广泛的适应能力。但是，ASIC 架构的缺点也同样明显，它的灵活性和扩展性不够，开发费用高，开发周期太长，一般耗时接近 2 年。

虽然研发成本较高，灵活性受限制、无法支持太多的功能，但其性能具有天然优势，非常适合应用于模式简单、对吞吐量和时延指标要求较高的电信级大流量的处理。

### 3. NP架构

NP可以说是介于以上两者之间的技术，NP架构是专门为处理网络流量而设计的处理器，其体系结构和指令集对于防火墙常用的包过滤、转发等算法和操作都进行了专门的优化，可以高效地完成TCP/IP协议栈的常用操作，并对网络流量进行快速的并发处理。硬件结构设计也大多采用高速的接口技术和总线规范，具有较高的I/O能力。

它可以构建一种硬件加速的完全可编程的架构，这种架构的软硬件都易于升级，软件可以支持新的标准和协议，硬件设计支持更高网络速度，从而使产品的生命周期更长。由于防火墙处理的就是网络数据包，所以基于NP架构的防火墙与X86架构的防火墙相比，性能得到了很大的提高。

NP通过专门的指令集和配套的软件开发系统，提供强大的编程能力，因而便于开发应用，支持可扩展的服务，而且研制周期短，成本较低。但是，相比较于X86架构，由于应用开发、功能扩展受到NP的配套软件的限制，基于NP技术的防火墙的灵活性要差一些。由于依赖软件环境，在性能方面NP不如ASIC。NP架构开发的难度和灵活性都介于ASIC和X86构架之间。应该说，NP是X86架构和ASIC之间的一个折中。

可以看出，X86、NP和ASIC各有优缺点。X86架构灵活性最高，新功能、新模块扩展容易，但性能肯定满足不了千兆需要。ASIC架构性能最高，千兆、万兆吞吐速率均可实现，但灵活性最低，定型后再扩展十分困难。NP架构则介于两者之间，性能可满足千兆需要，同时也具有一定的灵活性。

硬件防火墙一般至少应具备WAN、LAN和DMZ端口，分别接内网、外网和DMZ非军事化区，现在一些新的硬件防火墙往往扩展了端口，常见四端口防火墙一般将第四个端口作为配置口、管理端口，很多高性能的防火墙还可以进一步扩展其他端口数目。

### 4. 防火墙的配置端口

防火墙的控制端口通常为Console端口，防火墙的初始配置也是通过控制端口(Console)与PC(通常是笔记本电脑)的串口(RS-232)连接，再通过Windows系统自带的超级终端(HyperTerminal)程序进行选项配置。防火墙的初始配置物理连接与交换机初始配置连接方法一样，如图1-11所示。




图1-11　防火墙的配置端口

### 5. 防火墙的 LAN和 WAN端口

所谓防火墙就是在内部网和外部网之间构造的保护屏障，保护内部网免受来自外部网络中非法用户的侵入，从而实现保护内部网络用户安全的目的。一般网络分成内网和外网，也就是 LAN 和 WAN，因此所有的防火墙设备一般都具有区分内部和外部网络的两个端口：LAN 端口和 WAN 端口，如图 1-12 所示。

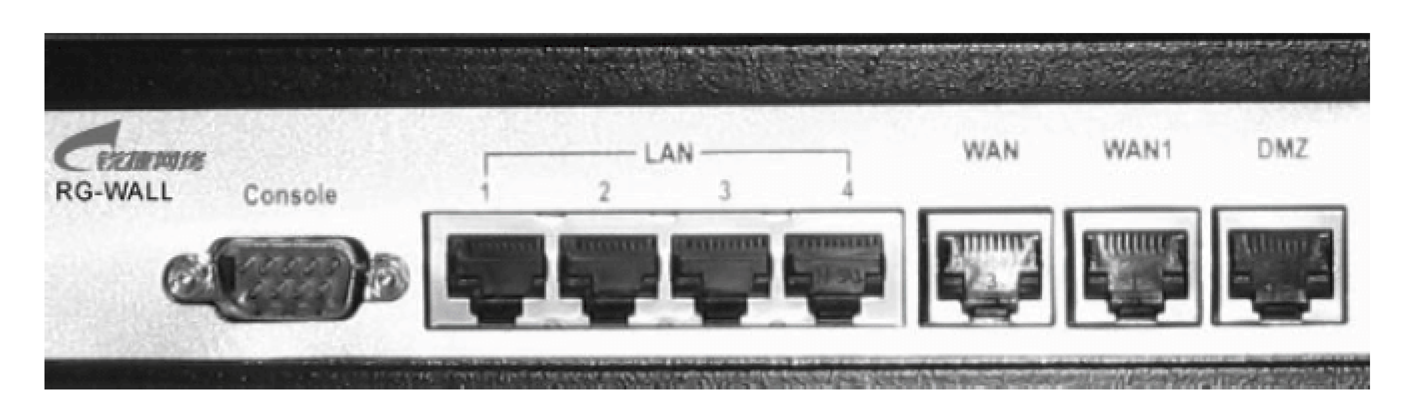



图 1-12　防火墙的 LAN、WAN 和 DMZ 端口

在防火墙默认情况下，为了保护内网，因此 LAN 端口一般连接的是受保护的网络区域。防火墙一般的策略是禁止外网访问内网，许可内网访问外网，因此 WAN 端口一般连接的是不受保护、不安全的网络区域。

因此当有 1 台 FTP 服务器，禁止被外部网络访问时，必须安装在 LAN 端口所连接的网络区域。当有 1 台 Web 服务器，需要被外网访问，并且，也被内网访问的时候，那么，有两种方法：一种是放在 LAN 中，一种是放在 DMZ。但如果这个服务器能被外网所访问，那么，就意味着这个服务器已经处于不可信任的状态，这个服务器就不能（主动）访问内网。

### 6. 防火墙的 DMZ端口

大多数的硬件防火墙设备上，都具有 DMZ 端口，如图 1-12 所示。DMZ 是 demilitarized zone 的缩写，中文名称为“隔离区”，也称“非军事化区”。

DMZ 端口是为了解决安装防火墙后，外部网络不能访问内部网络对外公共服务器的连接问题，而设立的一个非安全系统与安全系统之间的缓冲区，这个缓冲区位于企业内部网络和外部网络之间的小网络区域内，在这个小网络区域内可以放置一些必须公开的服务器设施，如企业 Web 服务器、FTP 服务器和论坛等，外部网络可以直接访问而不受防火墙的安全控制影响。

## 1.7　防火墙硬件参数

防火墙硬件参数是指设备使用的处理器类型或芯片及架构主频、内存容量、闪存容量、网络接口、存储容量类型等数据。此外专业级防火墙在选购时，还需要考虑以下技术指标。

### 1. 并发连接数

并发连接数是衡量防火墙性能的一个重要指标。在目前市面上常见防火墙设备的说明书中可以看到，从低端设备的 500、1000 个并发连接，一直到高端设备的数万、数十万个

并发连接，存在着好几个数量级的差异。那么，并发连接数究竟是一个什么概念呢？它的大小会对用户的日常使用产生什么影响呢？

要了解并发连接数，首先需要明白一个概念，那就是“会话”。这个“会话”可不是平时的谈话，但是可以用平时的谈话来理解，两个人在谈话时，你一句，我一句，一问一答，把它称为一次对话，或者叫会话。同样，在用计算机工作时，打开的一个窗口或一个 Web 页面，也可以把它叫做一个“会话”，扩展到一个局域网里面，所有用户要通过防火墙上网，要打开很多个窗口或 Web 页面(即会话)，那么，这个防火墙所能处理的最大会话数量，就是“并发连接数”。

并发连接数是指防火墙或代理服务器对其业务信息流的处理能力，是防火墙能够同时处理的点对点连接的最大数目，它反映出防火墙设备对多个连接的访问控制能力和连接状态跟踪能力，这个参数的大小直接影响到防火墙所能支持的最大信息点数。

### 2. 吞吐量

网络中的数据是由一个个数据包组成的，防火墙对每个数据包的处理要耗费资源。吞吐量是指在没有帧丢失的情况下，设备能够接受的最大速率。其测试方法是：在测试中以一定速率发送一定数量的帧，并计算待测设备传输的帧，如果发送的帧与接收的帧数量相等，那么就将发送速率提高并重新测试；如果接收帧少于发送帧则降低发送速率重新测试，直至得出最终结果。吞吐量测试结果以比特/秒或字节/秒为单位表示。

吞吐量和报文转发率是关系防火墙应用的主要指标，一般采用 FDT(Full Duplex Throughput)来衡量，指标准的 64 字节数据包的全双工吞吐量，该指标既包括吞吐量指标也涵盖了报文转发率指标。

吞吐量的大小主要由防火墙内网卡及程序算法的效率决定，尤其是程序算法，会使防火墙系统进行大量运算，通信量大打折扣。因此，大多数防火墙虽号称 100M 防火墙，由于其算法依靠软件实现，通信量远远没有达到 100M，实际只有 10～20M。纯硬件防火墙，由于采用硬件芯片进行运算，因此吞吐量可以达到线速 90～95M，从而是真正的 100M 防火墙。

对于中小型企业来讲，选择吞吐量为百兆级的防火墙即可满足需要，而对于电信、金融、保险等大公司大企业部门就需要采用吞吐量为千兆级的防火墙产品。

### 3. 用户数限制

防火墙的用户数限制分为固定限制用户数和无用户数限制两种。前者比如 SOHO 型防火墙一般支持几十到几百个用户不等，而无用户数限制大多用于大的部门或公司。要注意的是，用户数和并发连接数是完全不同的两个概念，并发连接数是指防火墙的最大会话数(或进程)，每个用户可以在一个时间里产生很多的连接，在购买产品时要区分这两个概念。

### 4. VPN 支持

虚拟专用网络(Virtual Private Network，VPN)可以理解成是虚拟出来的企业内部专线。它可以通过特殊的加密的通信协议在连接在 Internet 上不同地方的两个或多个企业内部网之间建立一条专有的通信线路，就好比是架设了一条专线一样，但是它并不需要

真正地去铺设光缆之类的物理线路。这就好比去电信局申请专线，但是不用给铺设线路的费用，也不用购买路由器等硬件设备。目前，绝大部分防火墙产品都支持 VPN 功能，但也有少部分不支持，建议在选购时注意此参数。

### 5. 安全过滤带宽

安全过滤带宽是指防火墙在某种加密算法标准下，如 DES(56 位)或 3DES(168 位)下的整体过滤性能。它是相对于明文带宽提出的。一般来说，防火墙总的吞吐量越大，其对应的安全过滤带宽越高。

# 第 2 章 防火墙设备实践操作技术

## 2.1 防火墙初始化配置

### 【实验名称】

防火墙初始化配置。

### 【实验目的】

登录防火墙，并使用初始化向导配置防火墙基本功能。

### 【背景描述】

某企业为了提高网络的安全性，购买了一台 RG-WALL 60 防火墙。现在需要登录防火墙并对其进行配置，使其满足基本的网络安全需求。

### 【需求分析】

防火墙的初始化向导可以帮助用户在防火墙第一次上线前进行基本功能的配置。

### 【实验拓扑】

如图 2-1 所示的网络拓扑，是企业为了提高网络的安全，规划的公司安全网络拓扑规划图，希望实现网络的安全访问控制功能。



图 2-1 某公司使用防火墙规划的安全网络拓扑图

### 【实验设备】

防火墙 1 台
PC 1 台

### 【预备知识】

- 网络基础知识。
- 防火墙基础知识。

### 【实验原理】

防火墙使用安全登录方式，只有通过严格的身份认证后，才能对防火墙进行管理。登录防火墙后，初始化向导可以帮助用户在防火墙第一次上线前进行基本功能配置。

## 【实验步骤】

### 1. 安装管理员证书

管理员证书存放在防火墙软件配套光盘中的 Admin Cert 文件夹中，如图 2-2 所示。




图 2-2　软件配套光盘中的管理员证书

双击 admin. p12 文件，该文件将初始 Windows 的证书导入向导，打开“欢迎使用证书导入向导”面板，单击“下一步”按钮，如图 2-3 所示。

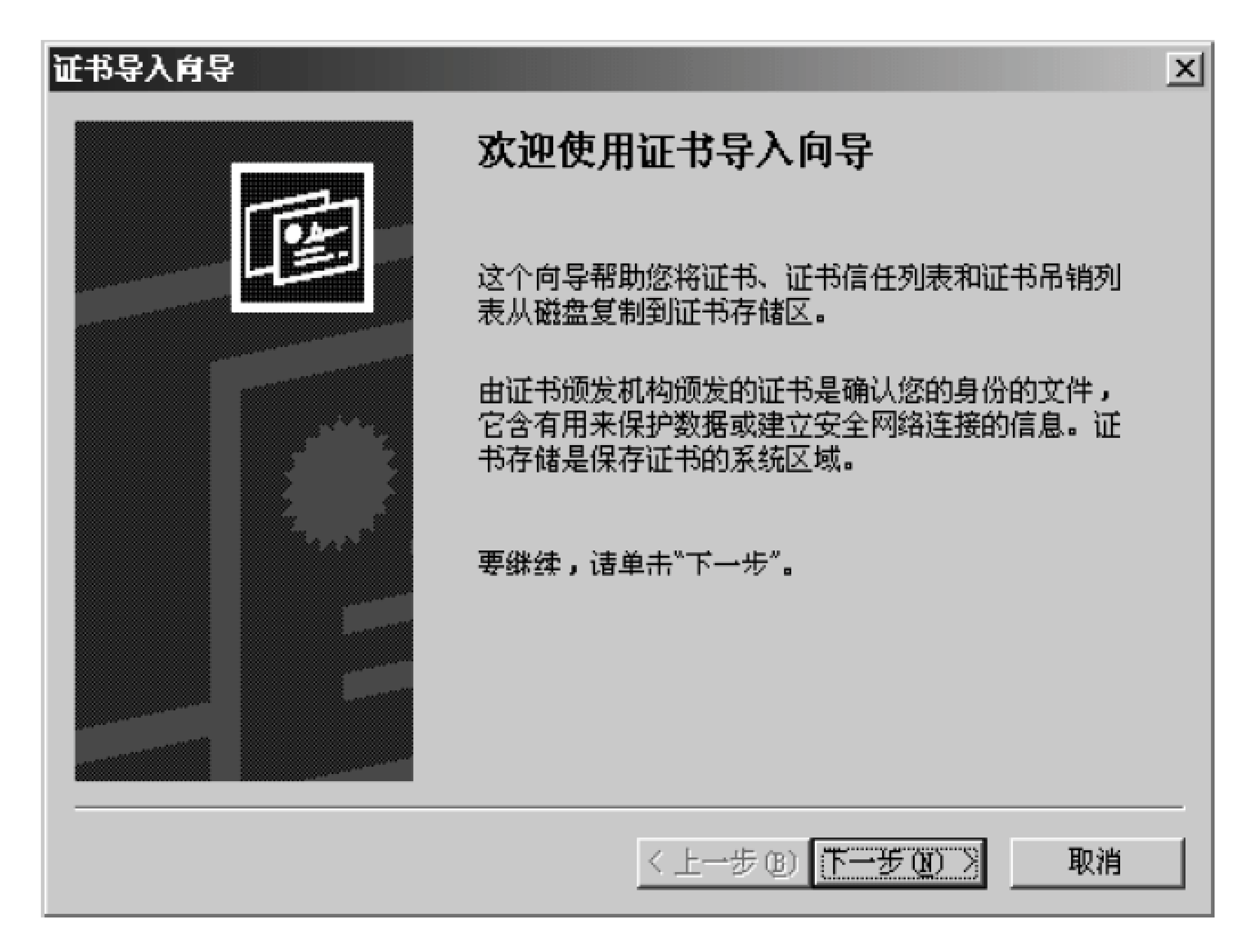



图 2-3　导入管理员证书

指定证书所在的路径，单击“下一步”按钮，如图 2-4 所示。

输入导入证书时使用的密码，密码为 123456，单击“下一步”按钮，如图 2-5 所示。

选择证书的存放位置，选中“根据证书类型，自动选择证书存储区”单选按钮，单击“下一步”按钮，如图 2-6 所示。

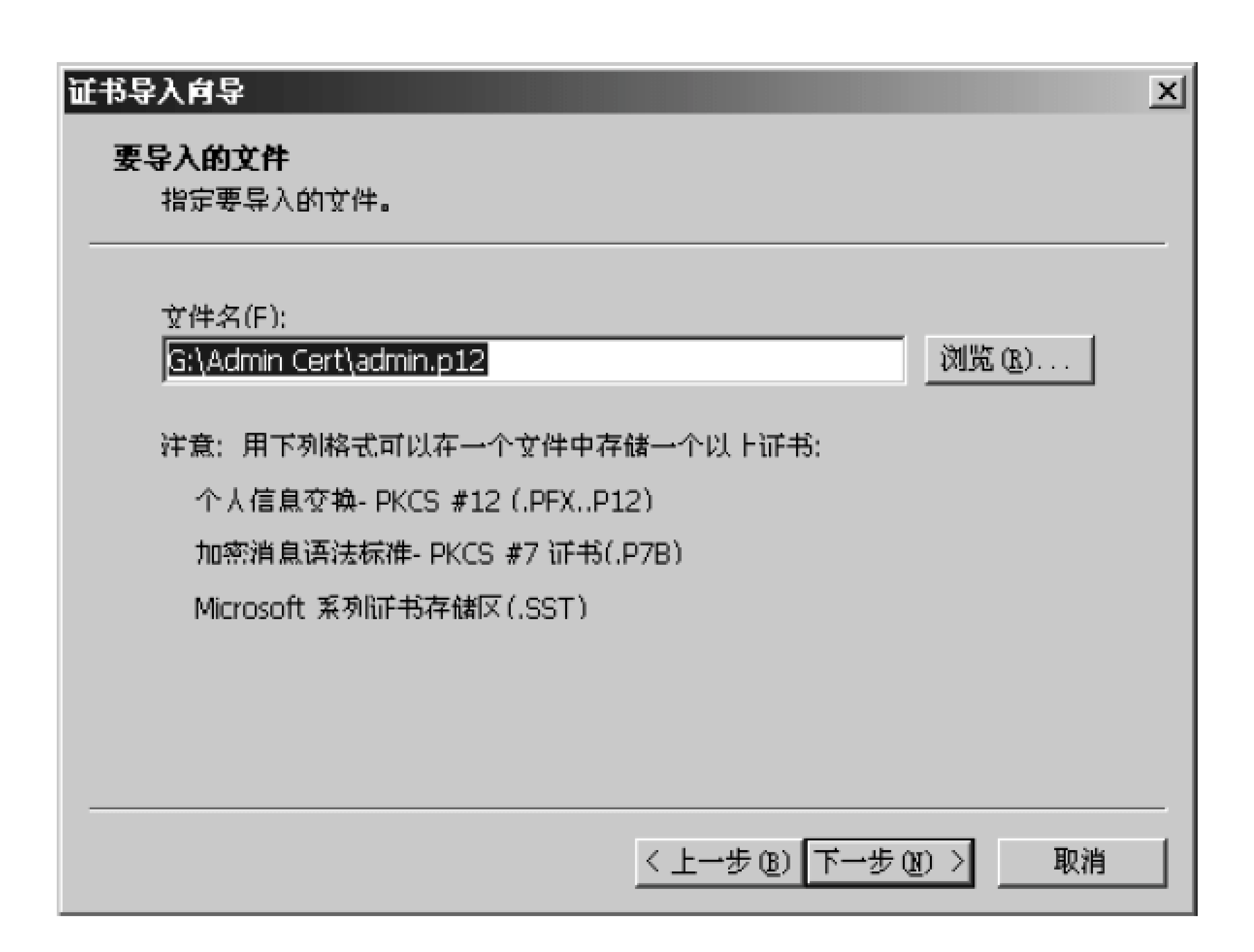



图 2-4　指定证书所在的路径

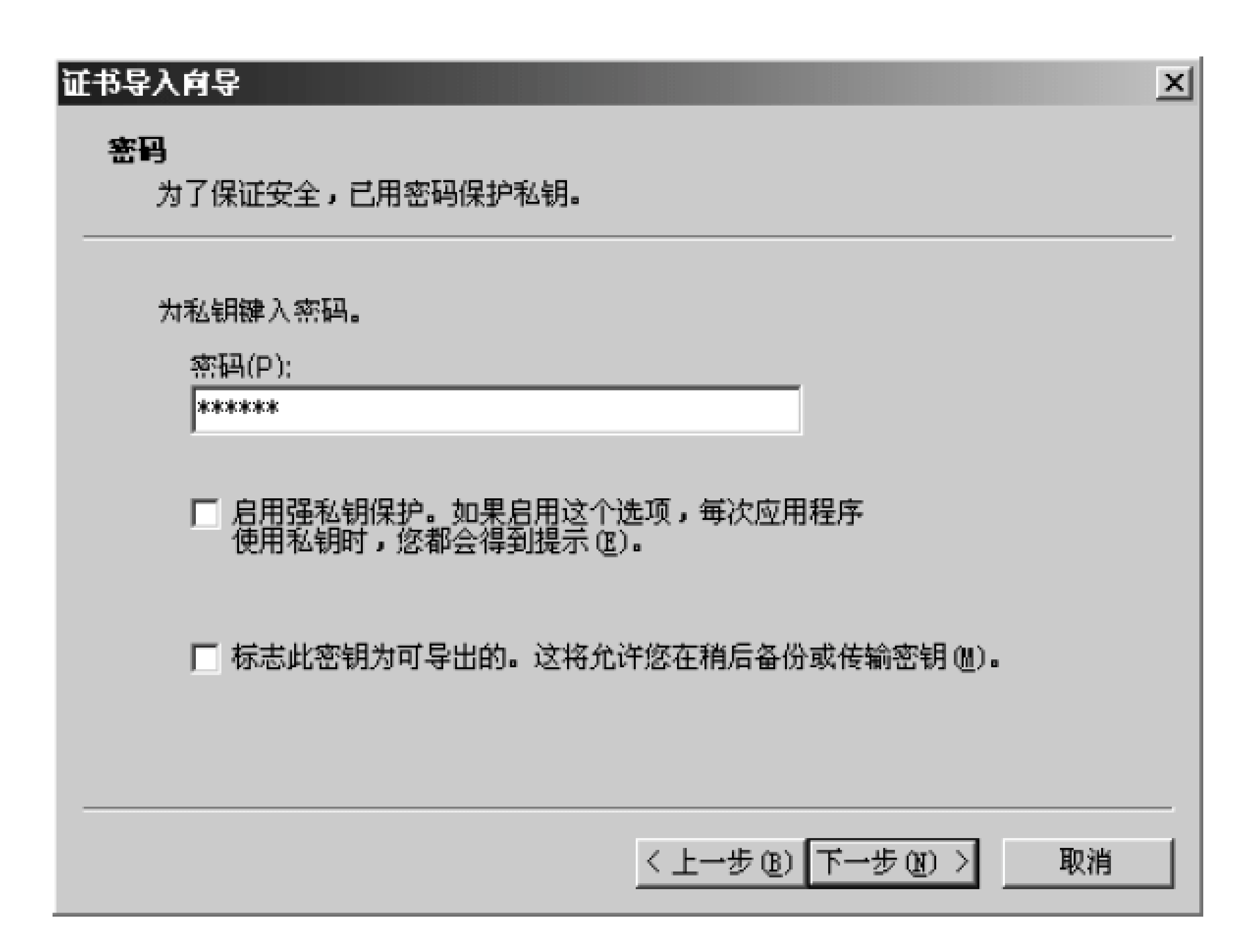



图 2-5　输入导入证书的默认密码




图 2-6　选择证书的存放位置

单击"下一步"按钮，完成证书的导入，如图 2-7 所示。单击"完成"按钮，系统会提示证书导入成功，如图 2-8 所示。




图 2-7　完成证书的导入




图 2-8　证书导入成功提示

## 2 登录防火墙

防火墙出厂时，默认在 WAN 接口配置了一个 IP 地址，如 192.168.10.100/24，并且授权只允许 IP 地址为 192.168.10.200 的主机进行管理。如图 2-1 所示的网络连接拓扑图。

将管理主机的 IP 地址配置为 192.168.10.200/24，在 Web 浏览器的地址栏中输入 https://192.168.10.100:6666。注意，这里使用"https"，这样所有的管理流量都将通过 SSL 进行加密；并且端口号为 6666，这是使用文件证书登录防火墙时使用的端口。如果使用 USB-KEY 登录，端口号为 6667。

当使用 https://192.168.10.100:6666 登录防火墙时，防火墙将提示管理主机初始管理员证书，该证书就是之前导入的管理员证书，单击"确定"按钮，如图 2-9 所示。

之后 Windows 系统会提示验证防火墙的证书，单击"确定"按钮，如图 2-10 所示。




图 2-9　选择初始管理员证书

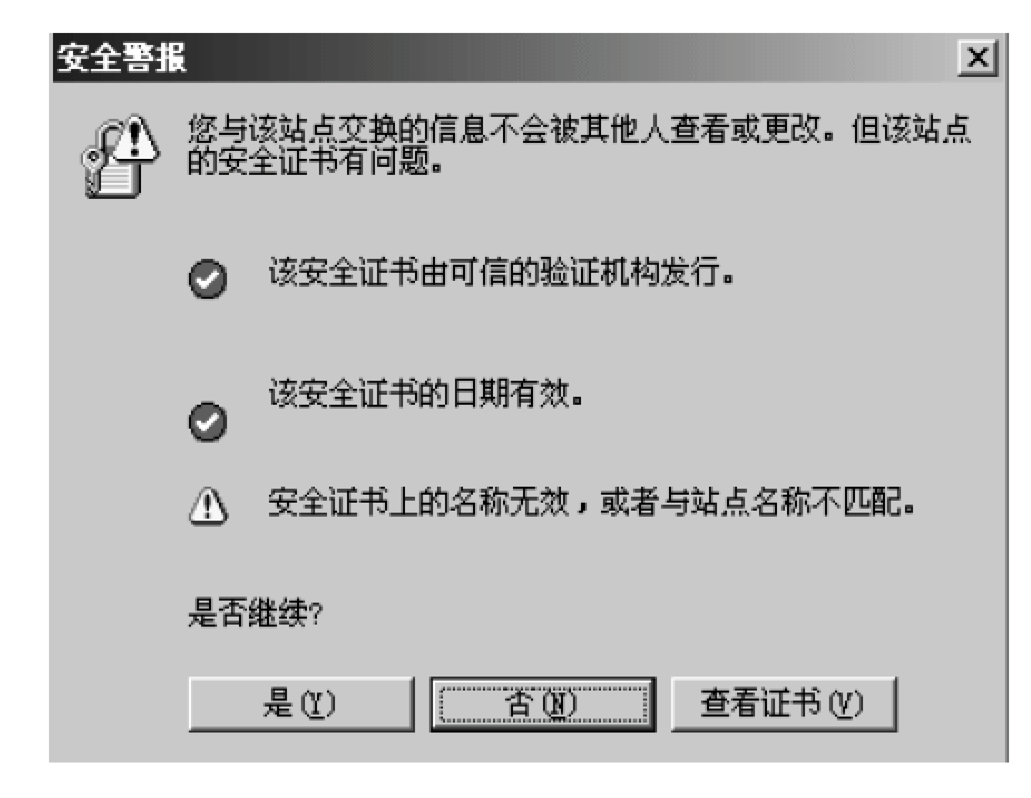



图 2-10　防火墙验证的证书

通过验证后，就可以进入防火墙的登录界面，如图 2-11 所示。

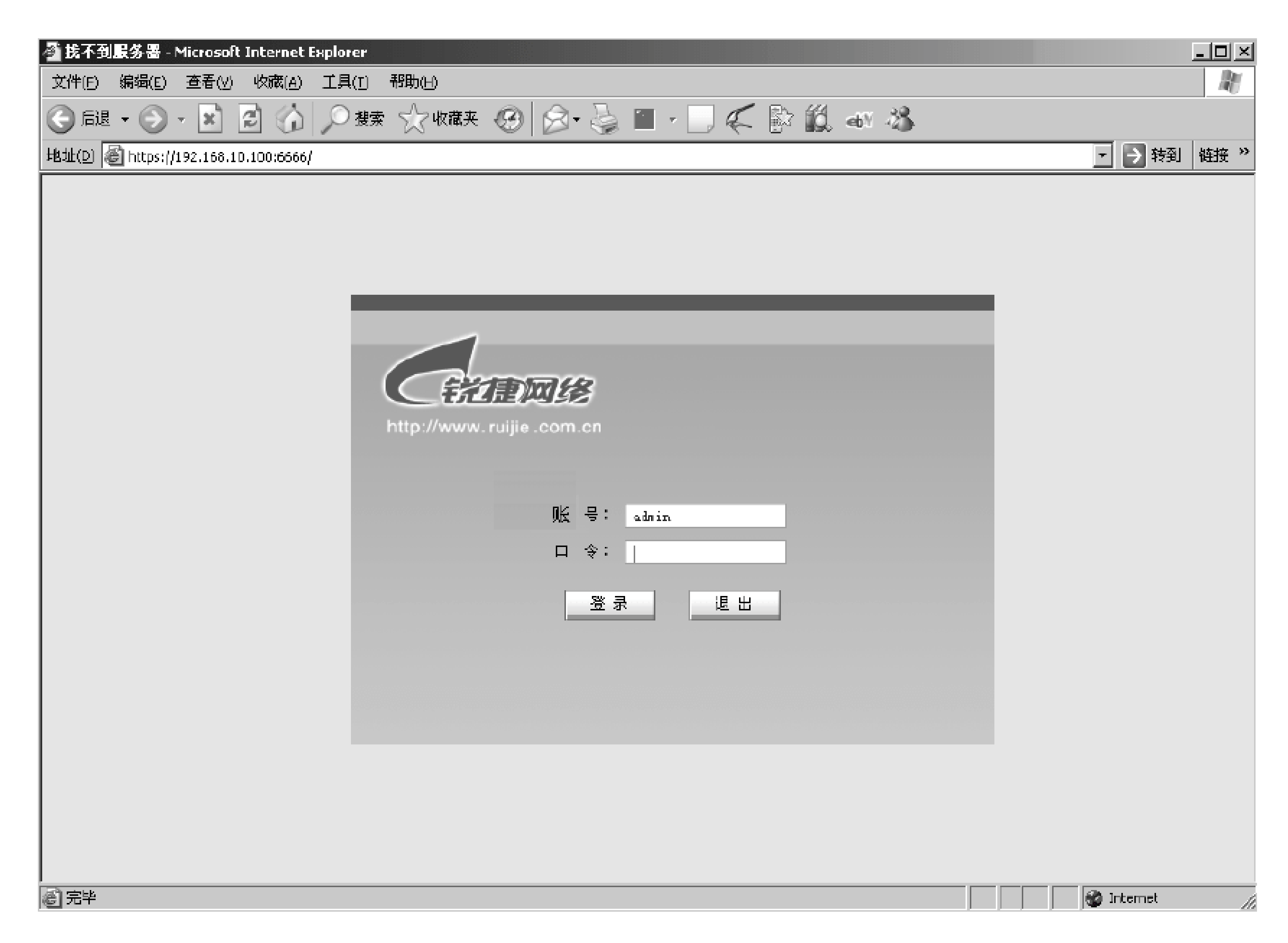



图 2-11　进入防火墙的登录界面

输入默认的用户名 admin，密码 firewall，登录防火墙，如图 2-12 所示。

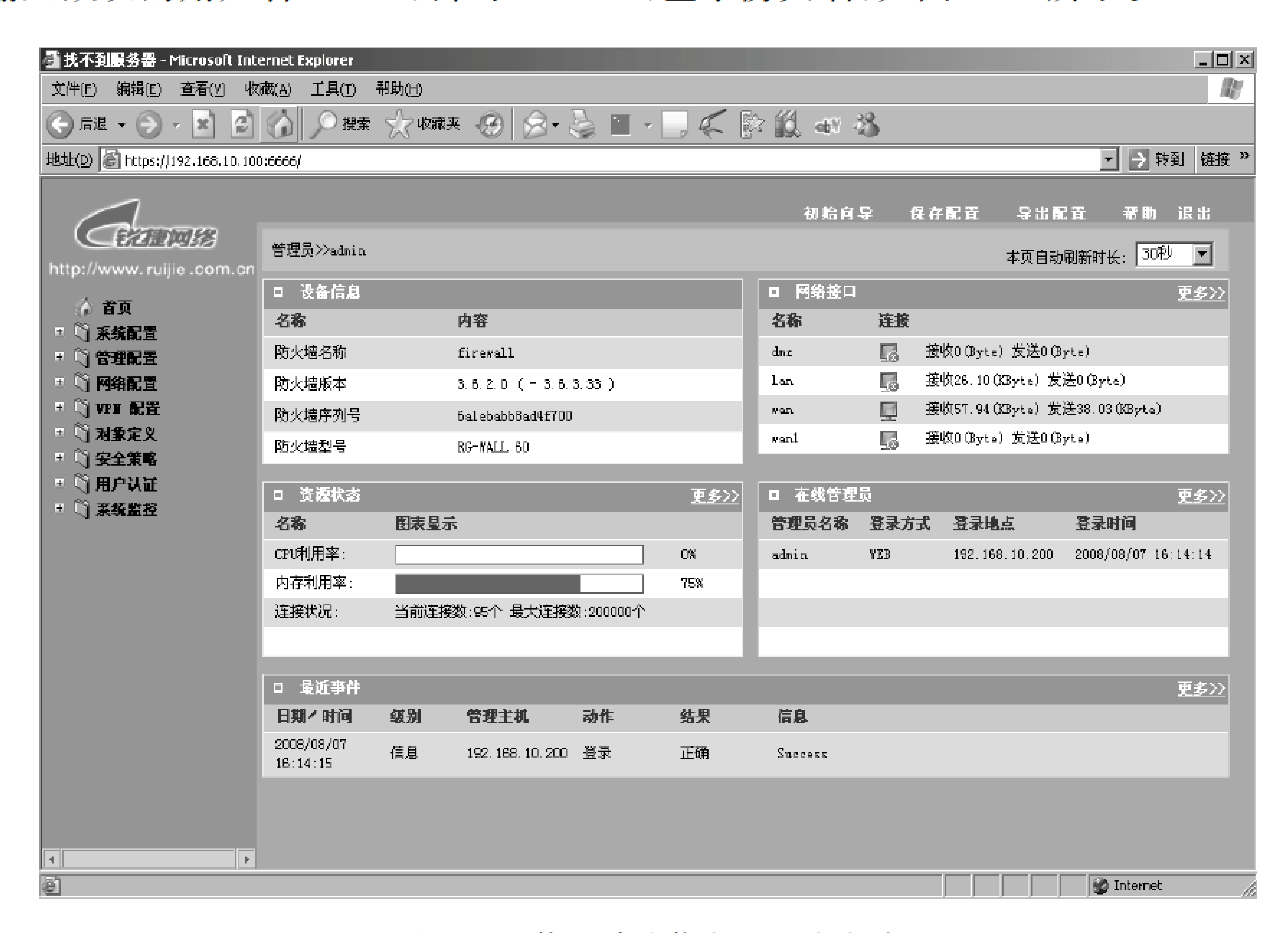



图 2-12　使用默认信息登录防火墙

### 3. 初始化向导 1——修改口令

进入防火墙配置页面后，单击右上方的“初始向导”按钮，进入防火墙的初始化向导。初始化向导的第 1 步是修改默认的管理员密码，如图 2-13 所示。




图 2-13　修改管理员密码

## 4. 初始化向导 2——工作模式

初始化向导的第 2 步是设置接口的工作模式。防火墙接口工作模式通常分为混合模式和路由模式，默认为路由模式。路由模式是指接口对报文进行路由转发；混合模式是指接口对报文进行透明桥接转发，如图 2-14 所示。




图 2-14　配置工作模式

## 5. 初始化向导 3——接口 IP

初始化向导的第 3 步是设置接口的 IP 地址和掩码信息，并且设置该地址是否作为管

理地址,是否允许连接在接口上的主机使用 ping 测试命令等选项,如图 2-15 所示。

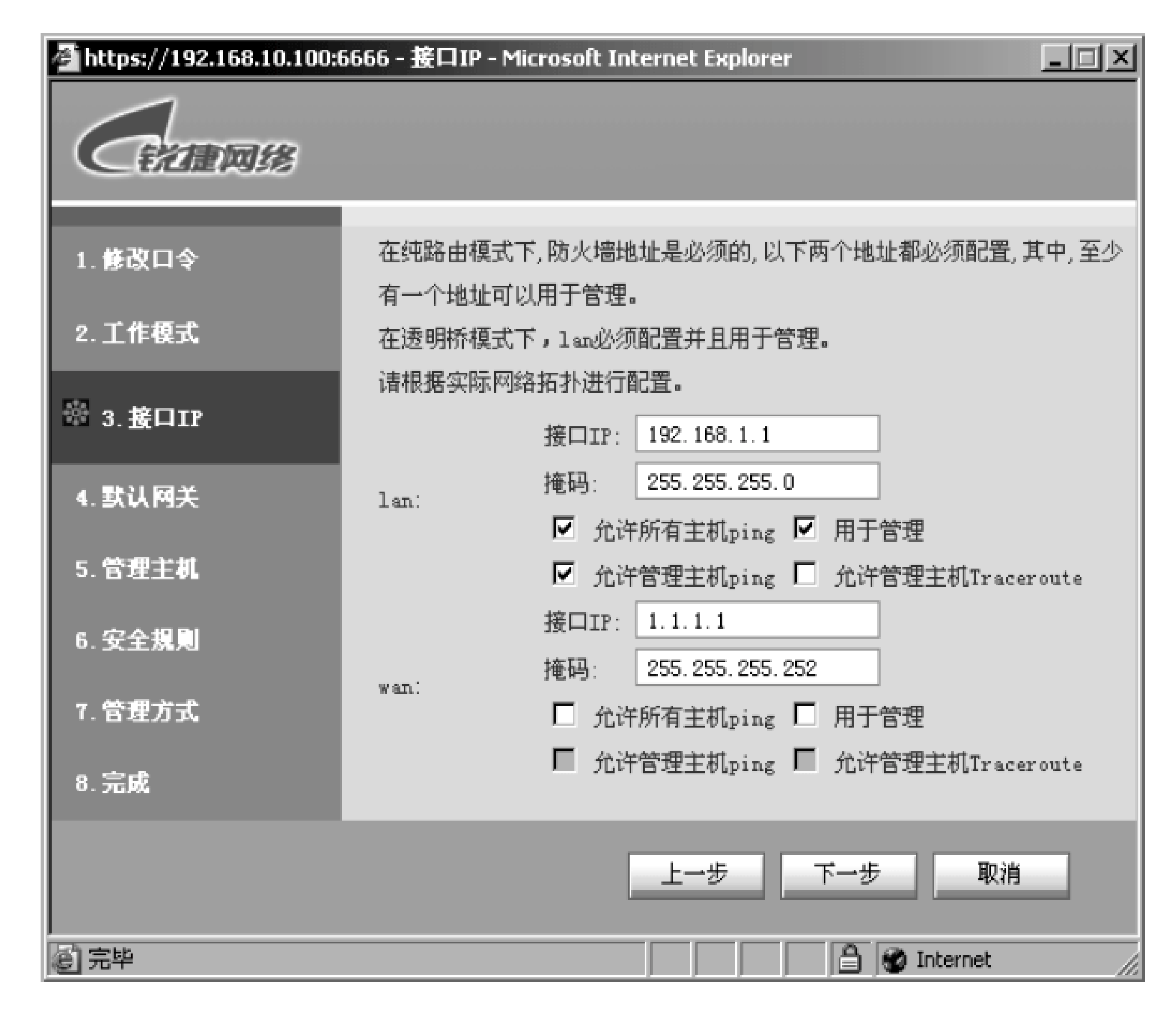



图 2-15　配置接口的 IP

### 6. 初始化向导 4——默认网关

初始化向导的第 4 步是设置防火墙的默认网关,通常这些都是 ISP 路由器的地址,如图 2-16 所示。




图 2-16　配置默认网关

### 7. 初始化向导 5——管理主机

初始化向导的第 5 步是设置管理主机,授权只有配置该地址的主机才可以对防火墙

进行管理。在配置界面上还可以添加多个管理主机。默认的管理主机为 192.168.1.254，如图 2-17 所示。




图 2-17　配置管理主机

## 8. 初始化向导 6——安全规则

初始化向导的第 6 步是添加安全规则，这里可以根据内部和外部的子网信息进行配置，如图 2-18 所示。




图 2-18　配置安全规则

### 9. 初始化向导 7——管理方式

初始化向导的第 7 步是设置管理防火墙的方式，这里可以选择 3 种方式：使用串口连接 Console 接口进行命令行管理；使用 Web 的 https 方式，即使用 SSH 加密连接进行 Web 方式管理，如图 2-19 所示。




图 2-19　配置管理方式

### 10. 初始化向导 8——完成向导

初始化向导的第 8 步是完成向导的配置，此时在页面上会显示之前步骤配置的结果，单击“完成”按钮，如图 2-20 所示。

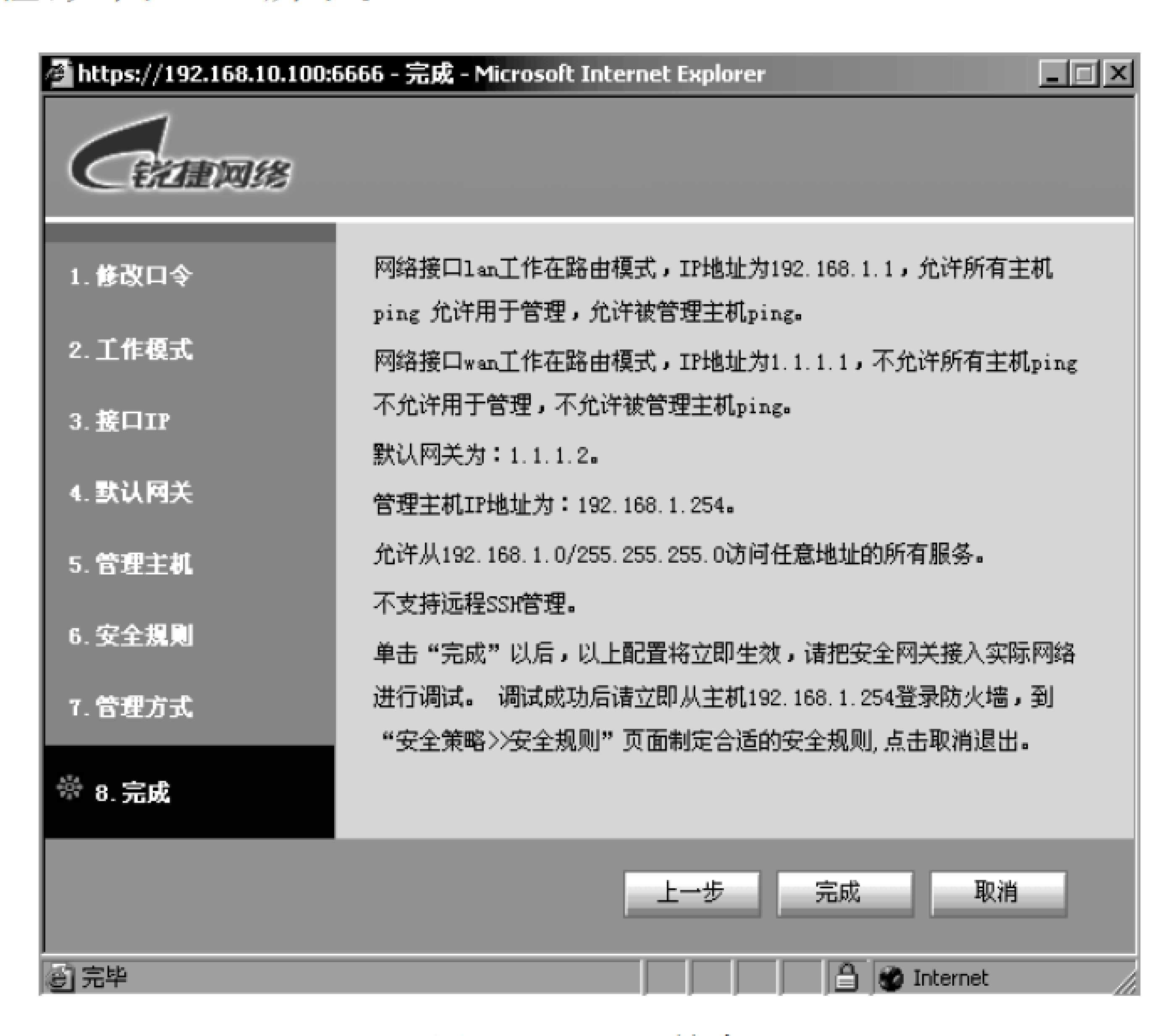



图 2-20　配置结束

**【注意事项】**

完成向导后，由于防火墙接口的地址、管理主机的地址已经改变，所以需要使用新的配置重新登录防火墙进行管理。

## 2.2　使用防火墙实现安全的访问控制

**【实验名称】**

使用防火墙实现安全的访问控制。

**【实验目的】**

利用防火墙的安全策略实现严格的访问控制。

**【背景描述】**

某企业网络的出口使用了一台防火墙作为接入 Internet 的设备，现在需要使用防火墙的安全策略来实现严格的访问控制，以允许必要的流量通过防火墙，并且阻止内网用户接入 Internet 上的未授权的访问。

企业内部网络使用的地址段为 100.1.1.0/24。公司经理的主机 IP 地址为 100.1.1.100/24，设计部的主机 IP 地址为 100.1.1.101/24～100.1.1.103/24，其他员工使用 100.1.1.2/24～100.1.1.99/24 范围内的地址。并且公司在公网上有一台 IP 地址为 200.1.1.1 的外部 FTP 服务器。

现在需要在防火墙上进行访问控制，使经理的主机可以访问 Internet 中的 Web 服务器和公司的外部 FTP 服务器，并能够使用邮件客户端（SMTP/POP3）收发邮件；设计部的主机可以访问 Internet 中的 Web 服务器和公司的外部 FTP 服务器；其他员工的主机只能访问公司的外部 FTP 服务器。

**【需求分析】**

企业网络需要对内部网络浏览 Internet 的流量进行限制，防火墙的安全策略（包过滤规则）可以满足这个需求，实现内部网络严格访问 Internet 的控制需求。

**【实验拓扑】**

如图 2-21 所示的网络拓扑，企业网络为了对内部网络浏览 Internet 的流量进行限制，配置防火墙的安全策略以实现企业内部网络安全访问 Internet 的控制需求。

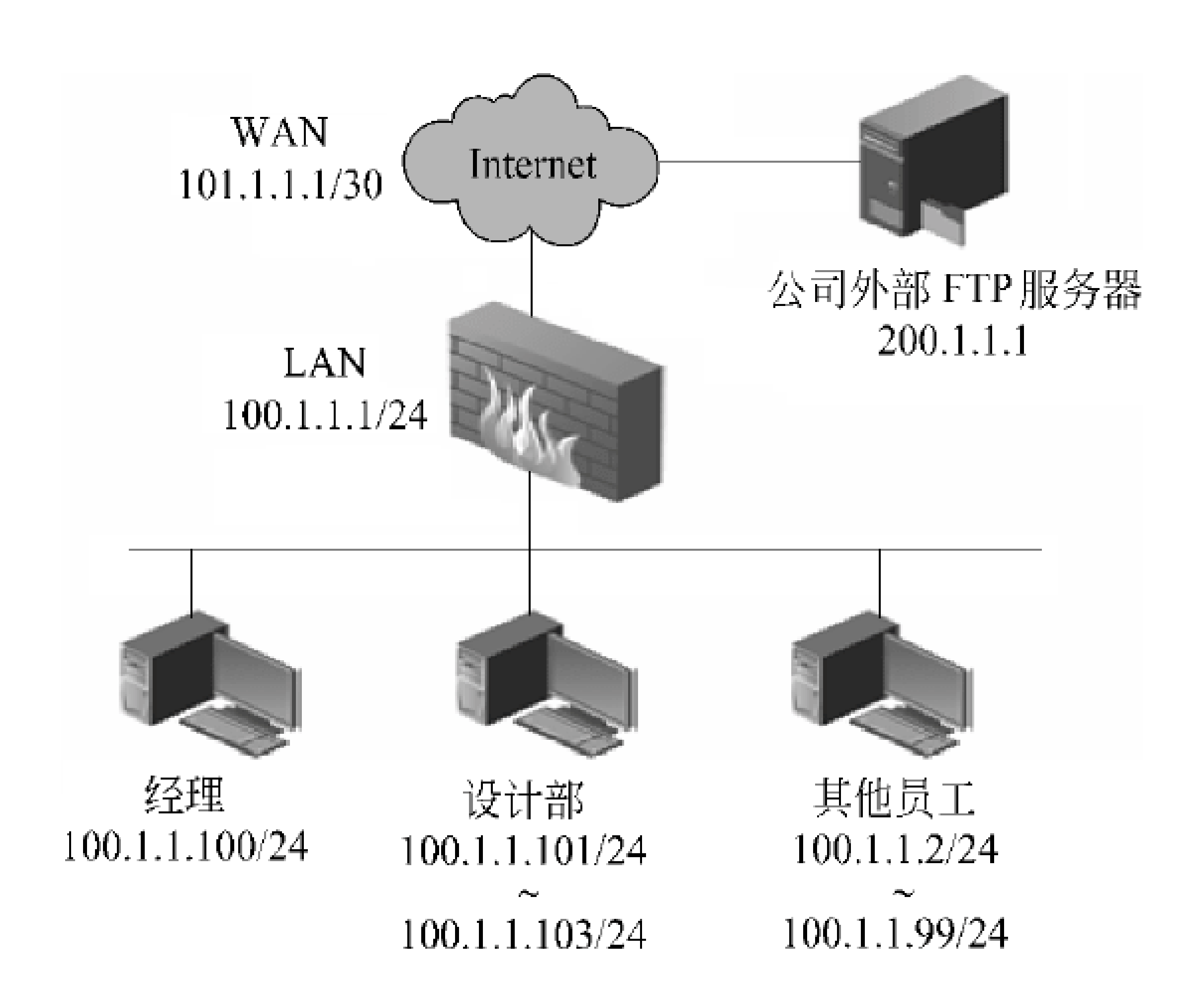



图 2-21　防火墙的安全策略配置规划拓扑图

## 【实验设备】

防火墙连接到 Internet 的链路

防火墙　　1 台

PC　　3 台

FTP 服务器　　1 台

## 【预备知识】

- 网络基础知识。
- 防火墙工作原理。

## 【实验原理】

实现访问控制是防火墙的基本功能，防火墙的安全策略（包过滤规则）可以根据数据包的源 IP 地址、目的 IP 地址、服务（端口号）等对通过防火墙的报文进行检测。

## 【实验步骤】

### 1. 配置防火墙接口的 IP 地址

如图 2-22 所示，进入防火墙的配置页面，即“网络配置≫接口 IP”页面，单击“添加”按钮，为接口添加 IP 地址。




| 网络接口 | 接口IP | 掩码 | 允许所有主机PING | 用于管理 | 允许管理主机PING | 允许管理主机Traceroute | 操作 |
|---|---|---|---|---|---|---|---|
| ADSL | 未启用 | | | | | | |
| DHCP | 未启用 | | | | | | |
| dmz | 1.1.1.1 | 255.0.0.0 | ✔ | ✔ | ✔ | ✔ | |

图 2-22　防火墙的 IP 配置页面

为防火墙的 LAN 接口配置 IP 地址及子网掩码,如图 2-23 所示。

| 添加、编辑接口IP | |
|---|---|
| * 网络接口: | lan |
| * 接口IP: | 100.1.1.1 |
| * 掩码: | 255.255.255.0 |
| 允许所有主机PING: | ☑ |
| 用于管理: | ☐ |
| 允许管理主机PING: | ☐ |
| 允许管理主机Traceroute: | ☐ |
| 确 定 | 取 消 |

图 2-23 配置防火墙 LAN 接口的 IP 地址

为防火墙的 WAN 接口配置 IP 地址及子网掩码,如图 2-24 所示。

| 添加、编辑接口IP | |
|---|---|
| * 网络接口: | wan |
| * 接口IP: | 101.1.1.1 |
| * 掩码: | 255.255.255.252 |
| 允许所有主机PING: | ☐ |
| 用于管理: | ☐ |
| 允许管理主机PING: | ☐ |
| 允许管理主机Traceroute: | ☐ |
| 确 定 | 取 消 |

图 2-24 配置防火墙 WAN 接口的 IP 地址

接口配置 IP 地址后的状态如图 2-25 所示。

| 网络接口 | 接口IP | 掩码 | 允许所有主机PING | 用于管理 | 允许管理主机PING | 允许管理主机Traceroute | 操作 |
|---|---|---|---|---|---|---|---|
| ADSL | 未启用 | | | | | | |
| DHCP | 未启用 | | | | | | |
| dmz | 1.1.1.1 | 255.0.0.0 | ✔ | ✔ | ✔ | ✔ | |
| lan | 100.1.1.1 | 255.255.255.0 | ✔ | ✖ | ✖ | ✖ | |
| wan | 101.1.1.1 | 255.255.255.252 | ✖ | ✖ | ✖ | ✖ | |

添 加 刷 新

图 2-25 防火墙接口配置的 IP 地址

## 2 配置针对经理的主机的访问控制规则

进入防火墙配置页面,即“安全策略≫安全规则”页面,单击页面上方的“包过滤规则”按钮,添加包过滤规则,如图 2-26 所示。

添加允许经理的主机访问 Internet 中的 Web 服务器的包过滤规则,如图 2-27 所示。

添加允许经理的主机进行 DNS 域名解析的访问规则,如图 2-28 所示。




图 2-26　防火墙的安全策略配置页面

包过滤规则维护
满足条件
规则名: manager_http （1-15位 字母、数字、减号、下划线的组合）
源地址: 手工输入 IP地址 100.1.1.100 掩 码 255.255.255.255
目的地址: IP地址 掩 码
服务: http
执行动作
动作: 允许 禁止　URL 过滤:
检查流入网口:　检查流出网口:
时间调度:　流量控制:
用户认证:　日志记录:
隧道名:　序号: 1
连接限制: 保护主机 保护服务 限制主机 限制服务
添加下一条　确 定　取 消

图 2-27　配置防火墙的包过滤规则

包过滤规则维护
满足条件
规则名: manager_dns （1-15位 字母、数字、减号、下划线的组合）
源地址: 手工输入 IP地址 100.1.1.100 掩 码 255.255.255.255
目的地址: any IP地址 掩 码
服务: dns
执行动作
动作: 允许 禁止　URL 过滤:
检查流入网口:　检查流出网口:
时间调度:　流量控制:
用户认证:　日志记录:
隧道名:　序号: 2
连接限制: 保护主机 保护服务 限制主机 限制服务
添加下一条　确 定　取 消

图 2-28　添加 DNS 域名解析的访问规则

添加允许经理的主机访问公司外部 FTP 服务器的访问规则，如图 2-29 所示。

添加允许经理的主机使用邮件客户端发送邮件（SMTP）的访问规则，如图 2-30 所示。

添加允许经理的主机使用邮件客户端接收邮件（POP3）的访问规则，如图 2-31 所示。



包过滤规则维护

满足条件

| | | | |
|---|---|---|---|
| 规则名： | manager_ftp （1-15位 字母、数字、减号、下划线的组合） | | |
| 源地址： | 手工输入<br>IP地址 100.1.1.100<br>掩 码 255.255.255.255 | 目的地址： | 手工输入<br>IP地址 200.1.1.1<br>掩 码 255.255.255.255 |
| 服务： | ftp | | |

执行动作

| | | | |
|---|---|---|---|
| 动作： | ⊙ 允许 ○ 禁止 | URL 过滤： | |
| 检查流入网口： | | 检查流出网口： | |
| 时间调度： | | 流量控制： | |
| 用户认证： | □ | 日志记录： | □ |
| 隧道名： | | 序号： | 3 |
| 连接限制： | □ 保护主机 □ 保护服务 □ 限制主机 □ 限制服务 | | |

添加下一条　确 定　取 消

图 2-29　添加 FTP 服务器的访问规则

包过滤规则维护

满足条件

| | | | |
|---|---|---|---|
| 规则名： | manager_send （1-15位 字母、数字、减号、下划线的组合） | | |
| 源地址： | 手工输入<br>IP地址 100.1.1.100<br>掩 码 255.255.255.255 | 目的地址： | <br>IP地址<br>掩 码 |
| 服务： | smtp | | |

执行动作

| | | | |
|---|---|---|---|
| 动作： | ⊙ 允许 ○ 禁止 | URL 过滤： | |
| 检查流入网口： | | 检查流出网口： | |
| 时间调度： | | 流量控制： | |
| 用户认证： | □ | 日志记录： | □ |
| 隧道名： | | 序号： | 4 |
| 连接限制： | □ 保护主机 □ 保护服务 □ 限制主机 □ 限制服务 | | |

添加下一条　确 定　取 消

图 2-30　添加发送邮件(SMTP)的访问规则

包过滤规则维护

满足条件

| | | | |
|---|---|---|---|
| 规则名： | manager_receive （1-15位 字母、数字、减号、下划线的组合） | | |
| 源地址： | 手工输入<br>IP地址 100.1.1.100<br>掩 码 255.255.255.255 | 目的地址： | any<br>IP地址<br>掩 码 |
| 服务： | pop3 | | |

执行动作

| | | | |
|---|---|---|---|
| 动作： | ⊙ 允许 ○ 禁止 | URL 过滤： | |
| 检查流入网口： | | 检查流出网口： | |
| 时间调度： | | 流量控制： | |
| 用户认证： | □ | 日志记录： | □ |
| 隧道名： | | 序号： | 5 |
| 连接限制： | □ 保护主机 □ 保护服务 □ 限制主机 □ 限制服务 | | |

添加下一条　确 定　取 消

图 2-31　添加接收邮件(POP3)的访问规则

### 3. 配置针对设计部的主机的访问控制规则

添加允许设计部的主机访问 Internet 中的 Web 服务器的访问规则，如图 2-32 所示。




图 2-32 添加 Web 服务器的访问规则

添加允许设计部的主机进行 DNS 域名解析的访问规则，如图 2-33 所示。

包过滤规则维护
满足条件
规则名: design_dns (1-15位 字母、数字、减号、下划线的组合)
源地址: 手工输入 IP地址 100.1.1.100 掩 码 255.255.255.252
目的地址: IP地址 掩 码
服务: dns
执行动作
动作: 允许 禁止
URL 过滤:
检查流入网口:
检查流出网口:
时间调度:
流量控制:
用户认证:
日志记录:
隧道名:
序号: 7
连接限制: 保护主机 保护服务 限制主机 限制服务
添加下一条 确 定 取 消

图 2-33 添加 DNS 域名解析的访问规则

添加允许设计部的主机访问公司外部 FTP 服务器的访问规则，如图 2-34 所示。

### 4. 配置针对其他员工的主机的访问控制规则

添加允许其他员工的主机访问公司外部 FTP 服务器的访问规则，如图 2-35 所示。

### 5. 访问规则

查看配置的访问规则，如图 2-36 所示。




图 2-34　添加 FTP 服务器的访问规则(1)




图 2-35　添加 FTP 服务器的访问规则(2)



安全策略>>安全规则　　跳转到 全部

| 序号 | 规则名 | 源地址 | 目的地址 | 服务 | 类型 | 选项 | 生效 |
|---|---|---|---|---|---|---|---|
| 1 | manager_http | 100.1.1.100 | any | http | ✓ | | ✔ |
| 2 | manager_dns | 100.1.1.100 | any | dns | ✓ | | ✔ |
| 3 | manager_ftp | 100.1.1.100 | 200.1.1.1 | ftp | ✓ | | ✔ |
| 4 | manager_send | 100.1.1.100 | any | smtp | ✓ | | ✔ |
| 5 | manager_receive | 100.1.1.100 | any | pop3 | ✓ | | ✔ |
| 6 | design_http | 100.1.1.100 | any | http | ✓ | | ✔ |
| 7 | design_dns | 100.1.1.100 | any | dns | ✓ | | ✔ |
| 8 | design_ftp | 100.1.1.100 | 200.1.1.1 | ftp | ✓ | | ✔ |
| 9 | employee_ftp | 100.1.1.0 | 200.1.1.1 | ftp | ✓ | | ✔ |

图 2-36　查看配置的访问规则

### 6. 验证测试

- 经理的主机可以访问 Internet 中的 Web 服务器和公司的外部 FTP 服务器，并能够使用邮件客户端(SMTP/POP3)收发邮件。
- 设计部的主机可以访问 Internet 中的 Web 服务器和公司的外部 FTP 服务器。
- 其他员工的主机只能访问公司的外部 FTP 服务器。

### 【注意事项】

- 防火墙的访问控制规则是按照顺序进行匹配的，如果数据流匹配到某条规则后，将不再进行后续规则的匹配。
- 默认情况下，防火墙拒绝所有没有明确允许的数据流通过。
- 在本实验中没有给出防火墙路由的配置，需要根据实际网络情况在防火墙上配置访问 Internet(通常使用默认路由)和内部不同子网络的路由。

## 2.3 使用防火墙实现安全 NAT

### 【实验名称】

使用防火墙实现安全 NAT。

### 【实验目的】

利用防火墙的安全 NAT 功能实现网络地址转换及访问控制。

### 【背景描述】

某企业网络的出口使用了一台防火墙作为接入 Internet 的设备，并且内部网络使用私有 IP 地址(RFC 1918)。现在需要使用防火墙的安全 NAT 功能在内部网络中使用私有地址的主机来访问 Internet 资源，并且还需要进行访问控制，只允许必要的流量通过防火墙。

企业内部网络使用的私有地址段为 10.1.1.0/24、10.1.2.0/24 和 10.1.3.0/24。经理使用的子网为 10.1.1.0/24，设计部使用的子网为 10.1.2.0/24，其他员工使用的子网为 10.1.3.0/24。并且公司在公网上有一台 IP 地址为 200.1.1.1 的外部 FTP 服务器。

现在需要在防火墙上进行访问控制，使经理的主机可以访问 Internet 中的 Web 服务器和公司的外部 FTP 服务器，并能够使用邮件客户端(SMTP/POP3)收发邮件；设计部的主机可以访问 Internet 中的 Web 服务器和公司的外部 FTP 服务器；其他员工的主机只能访问公司的外部 FTP 服务器。

### 【需求分析】

企业网络需要使用私有地址的内部网络访问 Internet，并且对内部网络浏览 Internet

的流量进行限制，防火墙的安全 NAT 功能可以同时满足这两个需求。

## 【实验拓扑】

如图 2-37 所示的网络拓扑，企业网络使用私有地址内部网络来访问 Internet，并且对内部网络浏览 Internet 的流量进行限制，配置防火墙的安全策略以实现企业内部网络安全访问控制需求。

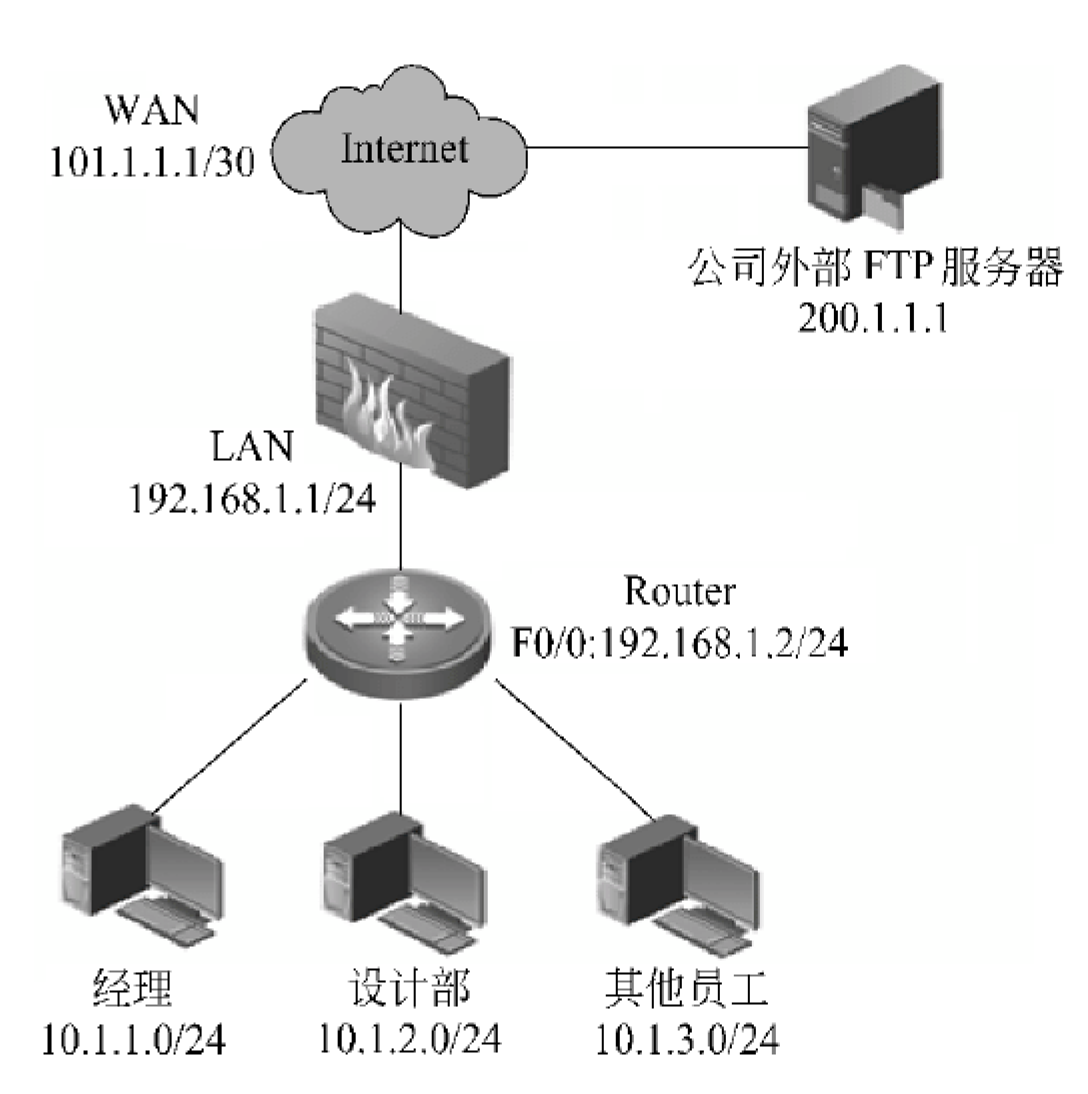



图 2-37 防火墙实现安全 NAT 网络规划拓扑图

## 【实验设备】

防火墙连接到 Internet 的链路

防火墙 1 台

路由器 1 台

PC 3 台

FTP 服务器 1 台

## 【预备知识】

- 网络基础知识。
- 防火墙的基础知识。

## 【实验原理】

实现安全的 NAT 地址转换是防火墙的基本功能，防火墙的安全 NAT 规则可以根据数据包的源 IP 地址、目的 IP 地址、服务(端口号)等对通过防火墙的报文进行检测，并进行必要的地址转换。

# 【实验步骤】

## 1. 配置防火墙接口的 IP 地址

如图 2-38 所示，进入防火墙的配置页面，即“网络配置≫接口 IP”页面，单击“添加”按钮，为接口添加 IP 地址。




图 2-38　防火墙的配置页面

为防火墙的 LAN 接口配置 IP 地址及子网掩码，如图 2-39 所示。

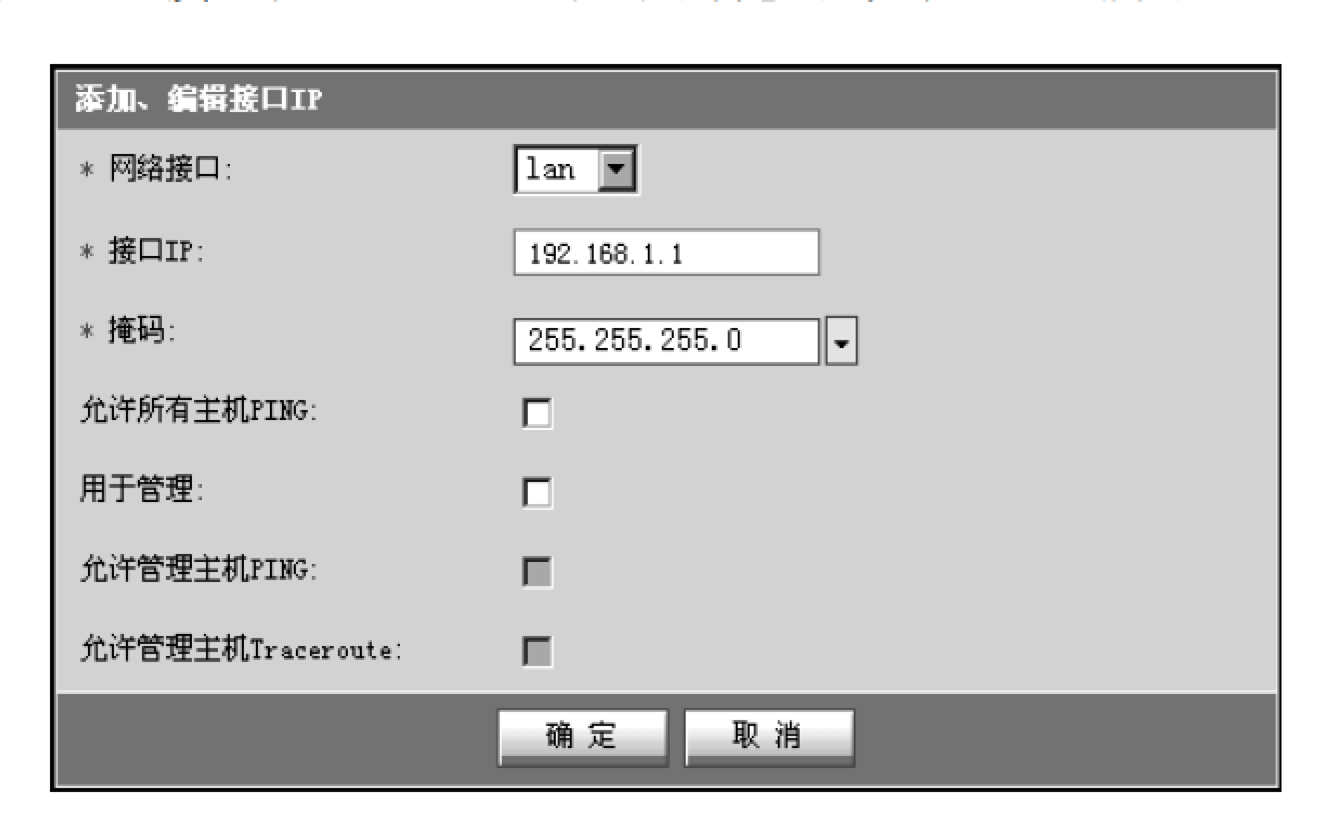



图 2-39　配置防火墙 LAN 接口的 IP 地址

为防火墙的 WAN 接口配置 IP 地址及子网掩码，如图 2-40 所示。

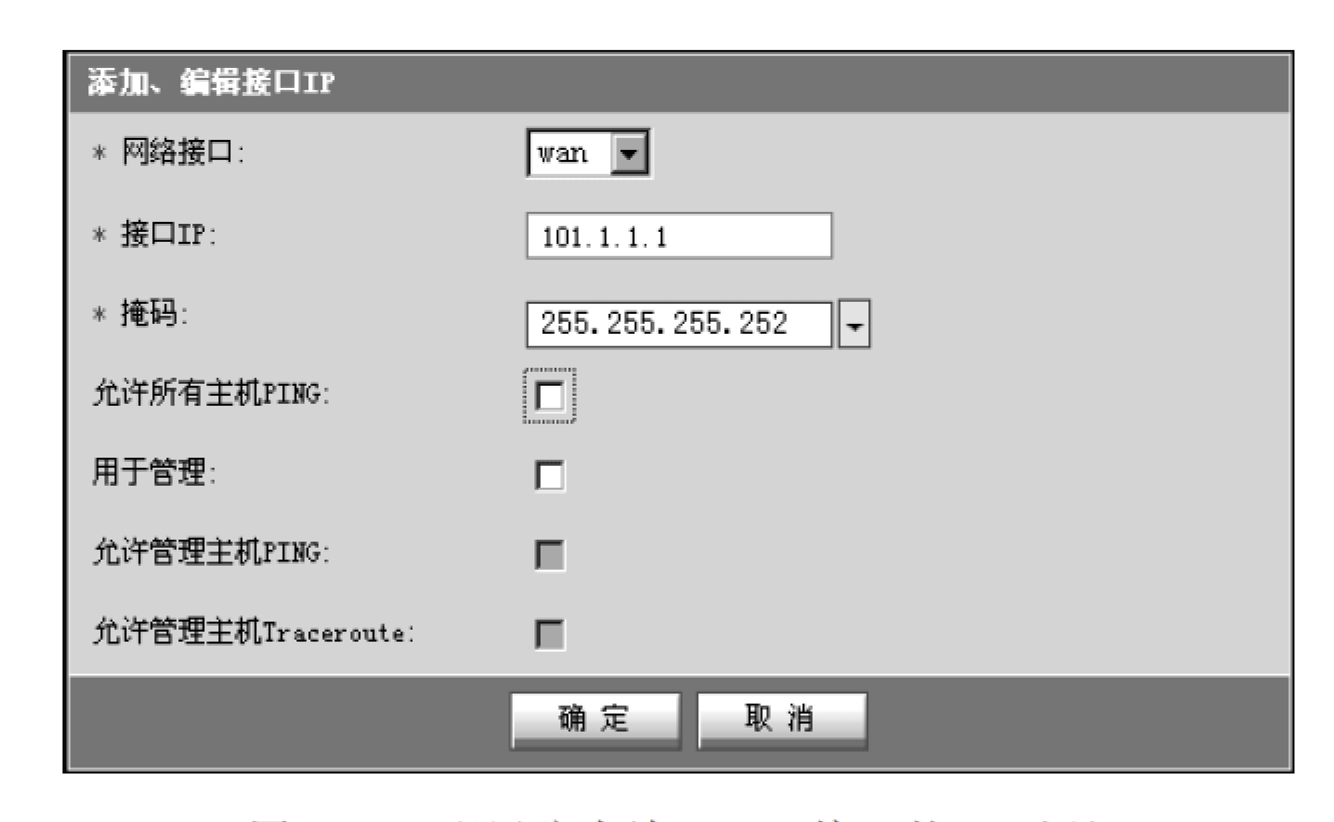



图 2-40　配置防火墙 WAN 接口的 IP 地址

接口配置 IP 地址后的状态如图 2-41 所示。

| 网络接口 | 接口IP | 掩码 | 允许所有主机PING | 用于管理 | 允许管理主机PING | 允许管理主机Traceroute | 操作 |
|---|---|---|---|---|---|---|---|
| ADSL | 未启用 | | | | | | |
| DHCP | 未启用 | | | | | | |
| dmz | 1.1.1.1 | 255.0.0.0 | ✔ | ✔ | ✔ | ✔ | |
| lan | 192.168.1.1 | 255.255.255.0 | ✖ | ✖ | ✖ | ✖ | |
| wan | 101.1.1.1 | 255.255.255.252 | ✖ | ✖ | ✖ | ✖ | |

添加　刷新

图 2-41　配置防火墙接口的 IP 地址

## 2 配置针对经理的主机的安全 NAT 规则

进入防火墙配置页面，即“安全策略≫安全规则”页面，单击页面上方的“NAT 规则”按钮，添加 NAT 规则，如图 2-42 所示。




图 2-42　配置防火墙的安全策略页面

添加允许经理的主机访问 Internet 中的 Web 服务器的 NAT 规则，如图 2-43 所示。

NAT规则维护

满足条件

| | | | |
|---|---|---|---|
| 规则名: | manager_http （1-15位 字母、数字、减号、下划线的组合） | | |
| 源地址: | 手工输入<br>IP地址 10.1.1.0<br>掩 码 255.255.255.0 | 目的地址: | any<br>IP地址<br>掩 码 |
| * 源地址转换为: | 101.1.1.1 | 服务: | http |

执行动作

| | | | |
|---|---|---|---|
| 检查流入网口: | lan | 检查流出网口: | wan |
| 时间调度: | | 流量控制: | |
| 用户认证: | ☐ | 日志记录: | ☐ |
| URL 过滤: | | 隧道名: | |
| *序号: | 1 | | |
| 连接限制: | ☐ 保护主机 ☐ 保护服务 ☐ 限制主机 ☐ 限制服务 | | |

添加下一条　确 定　取 消

图 2-43　添加 Web 服务器的 NAT 规则

添加允许经理的主机进行 DNS 域名解析的 NAT 规则，如图 2-44 所示。

添加允许经理的主机访问公司外部 FTP 服务器的 NAT 规则，如图 2-45 所示。

添加允许经理的主机使用邮件客户端发送邮件(SMTP)的 NAT 规则，如图 2-46 所示。




图 2-44　添加 DNS 域名解析的 NAT 规则

NAT规则维护
满足条件
规则名: manager_ftp （1-15位 字母、数字、减号、下划线的组合）
源地址: 手工输入 IP地址 10.1.1.0 掩 码 255.255.255.0
目的地址: 手工输入 IP地址 200.1.1.1 掩 码 255.255.255.255
* 源地址转换为: 101.1.1.1
服务: ftp
执行动作
检查流入网口: lan
检查流出网口: wan
时间调度:
流量控制:
用户认证:
日志记录:
URL 过滤:
隧道名:
*序号: 3
连接限制: 保护主机 保护服务 限制主机 限制服务
添加下一条 确 定 取 消

图 2-45　添加 FTP 服务器的 NAT 规则




图 2-46　添加发送邮件(SMTP)的 NAT 规则

添加允许经理的主机使用邮件客户端接收邮件(POP3)的 NAT 规则，如图 2-47 所示。


NAT规则维护

满足条件

规则名: manager_pop3 ( 1-15位 字母、数字、减号、下划线的组合 )

源地址: 手工输入　IP地址 10.1.1.0　掩 码 255.255.255.0

目的地址: any　IP地址　掩 码

* 源地址转换为: 101.1.1.1　服务: pop3

执行动作

检查流入网口: lan　检查流出网口: wan

时间调度:　流量控制:

用户认证: ☐　日志记录: ☐

URL 过滤:　隧道名:

*序号: 5

连接限制: ☐ 保护主机 ☐ 保护服务 ☐ 限制主机 ☐ 限制服务

添加下一条　确 定　取 消

图 2-47　添加接收邮件(POP3)的 NAT 规则

### 3. 配置针对设计部的主机的安全 NAT 规则

添加允许设计部的主机访问 Internet 中的 Web 服务器的 NAT 规则，如图 2-48 所示。

NAT规则维护

满足条件

规则名: design_http ( 1-15位 字母、数字、减号、下划线的组合 )

源地址: 手工输入　IP地址 10.1.2.0　掩 码 255.255.255.0

目的地址: any　IP地址　掩 码

* 源地址转换为: 101.1.1.1　服务: http

执行动作

检查流入网口: lan　检查流出网口: wan

时间调度:　流量控制:

用户认证: ☐　日志记录: ☐

URL 过滤:　隧道名:

*序号: 6

连接限制: ☐ 保护主机 ☐ 保护服务 ☐ 限制主机 ☐ 限制服务

添加下一条　确 定　取 消

图 2-48　配置访问 Internet 中的 Web 服务器的 NAT 规则

添加允许设计部的主机进行 DNS 域名解析的 NAT 规则，如图 2-49 所示。

添加允许设计部的主机访问公司外部 FTP 服务器的 NAT 规则，如图 2-50 所示。

### 4. 配置针对其他员工的主机的安全 NAT 规则

添加允许其他员工的主机访问公司外部 FTP 服务器的 NAT 规则，如图 2-51 所示。




图 2-49 添加 DNS 域名解析的 NAT 规则

NAT规则维护
满足条件
规则名: design_ftp （1-15位 字母、数字、减号、下划线的组合）
源地址: 手工输入 IP地址 10.1.2.0 掩 码 255.255.255.0
目的地址: 手工输入 IP地址 200.1.1.1 掩 码 255.255.255.255
* 源地址转换为: 101.1.1.1
服务: ftp
执行动作
检查流入网口: lan
检查流出网口: wan
时间调度:
流量控制:
用户认证:
日志记录:
URL 过滤:
隧道名:
*序号: 8
连接限制: 保护主机 保护服务 限制主机 限制服务
添加下一条 确 定 取 消

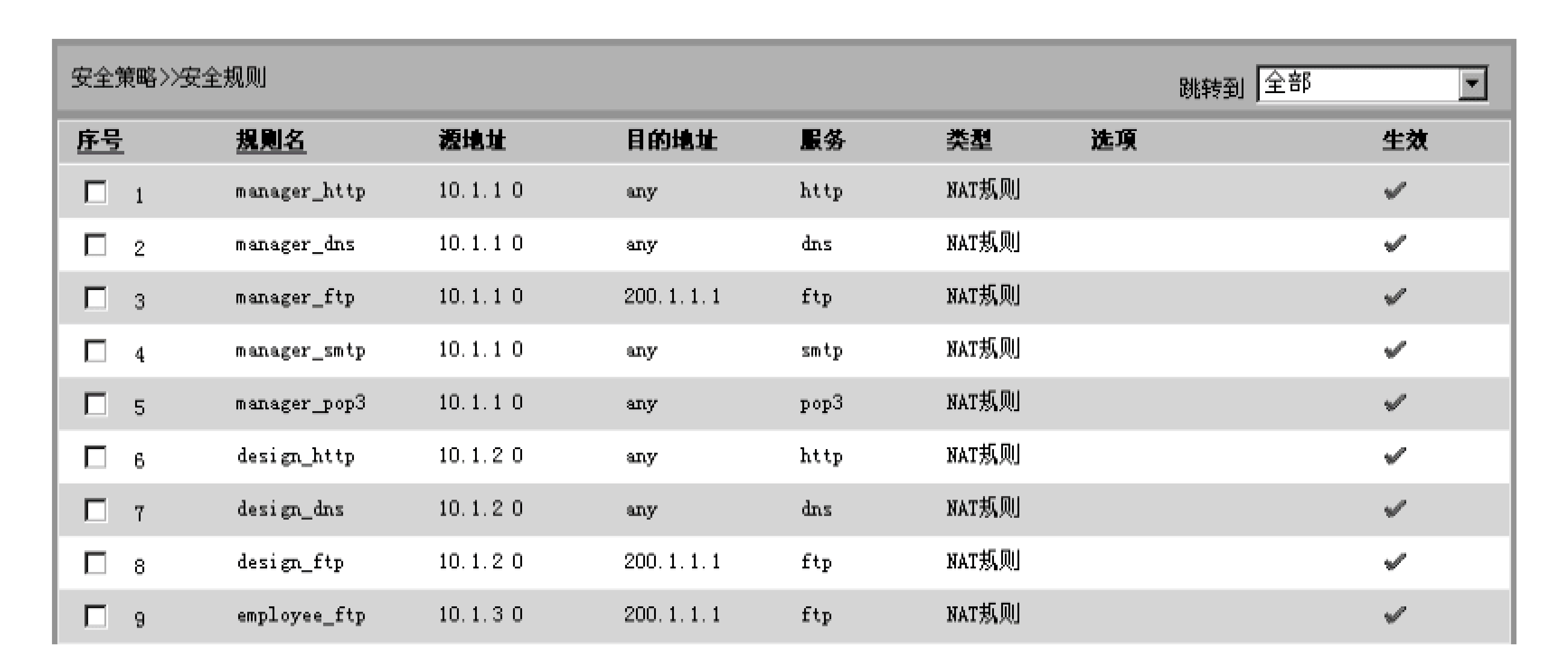
图 2-50 添加 FTP 服务器的 NAT 规则(1)




图 2-51 添加 FTP 服务器的 NAT 规则(2)

### 5. 访问规则

查看配置的访问规则,如图 2-52 所示。



安全策略>>安全规则　　跳转到 全部

| 序号 | 规则名 | 源地址 | 目的地址 | 服务 | 类型 | 选项 | 生效 |
|---|---|---|---|---|---|---|---|
| 1 | manager_http | 10.1.1.0 | any | http | NAT规则 | | ✔ |
| 2 | manager_dns | 10.1.1.0 | any | dns | NAT规则 | | ✔ |
| 3 | manager_ftp | 10.1.1.0 | 200.1.1.1 | ftp | NAT规则 | | ✔ |
| 4 | manager_smtp | 10.1.1.0 | any | smtp | NAT规则 | | ✔ |
| 5 | manager_pop3 | 10.1.1.0 | any | pop3 | NAT规则 | | ✔ |
| 6 | design_http | 10.1.2.0 | any | http | NAT规则 | | ✔ |
| 7 | design_dns | 10.1.2.0 | any | dns | NAT规则 | | ✔ |
| 8 | design_ftp | 10.1.2.0 | 200.1.1.1 | ftp | NAT规则 | | ✔ |
| 9 | employee_ftp | 10.1.3.0 | 200.1.1.1 | ftp | NAT规则 | | ✔ |

图 2-52　查看配置的访问规则

### 6. 验证测试

- 经理的主机可以访问 Internet 中的 Web 服务器和公司的外部 FTP 服务器,并能够使用邮件客户端(SMTP/POP3)收发邮件。
- 设计部的主机可以访问 Internet 中的 Web 服务器和公司的外部 FTP 服务器。
- 其他员工的主机只能访问公司的外部 FTP 服务器。

## 【注意事项】

- 防火墙的 NAT 规则是按照顺序进行匹配的,如果数据流匹配到某条规则后,将不再进行后续规则的匹配。
- 默认情况下,防火墙拒绝所有没有明确允许的数据流通过,并且不对其进行地址转换。
- 在本实验中没有给出防火墙路由的配置,需要根据实际网络情况在防火墙上配置访问 Internet(通常是默认路由)和内部网络的路由。
- 本实验没有给出内部网络中路由器的配置,为了实现网络的互通,需要在路由器上配置地址和相关路由信息。

# 2.4 配置防火墙地址绑定

## 【实验名称】

配置防火墙地址绑定。

## 【实验目的】

利用防火墙对上网用户的 IP 地址与 MAC 地址进行绑定。

## 【背景描述】

某企业网络管理员发现，一些用户经常盗用其他用户的 IP 地址，造成其他用户不能正常访问网络资源。

## 【需求分析】

企业要求必须在防火墙上解决该问题，避免盗用地址的情况再次出现。地址绑定技术是防止 IP 欺骗和防止盗用 IP 地址的有效手段。RG-WALL 防火墙提供自动探测 IP/MAC 地址对功能，可以减轻管理员手工收集 IP/MAC 地址对的工作量。

## 【实验拓扑】

如图 2-53 所示的网络拓扑，企业网络要求必须在防火墙上解决盗用地址的情况再次出现。地址绑定技术是防止 IP 欺骗和防止盗用 IP 地址的有效手段，配置防火墙的地址绑定以实现企业内部网络安全访问控制需求。

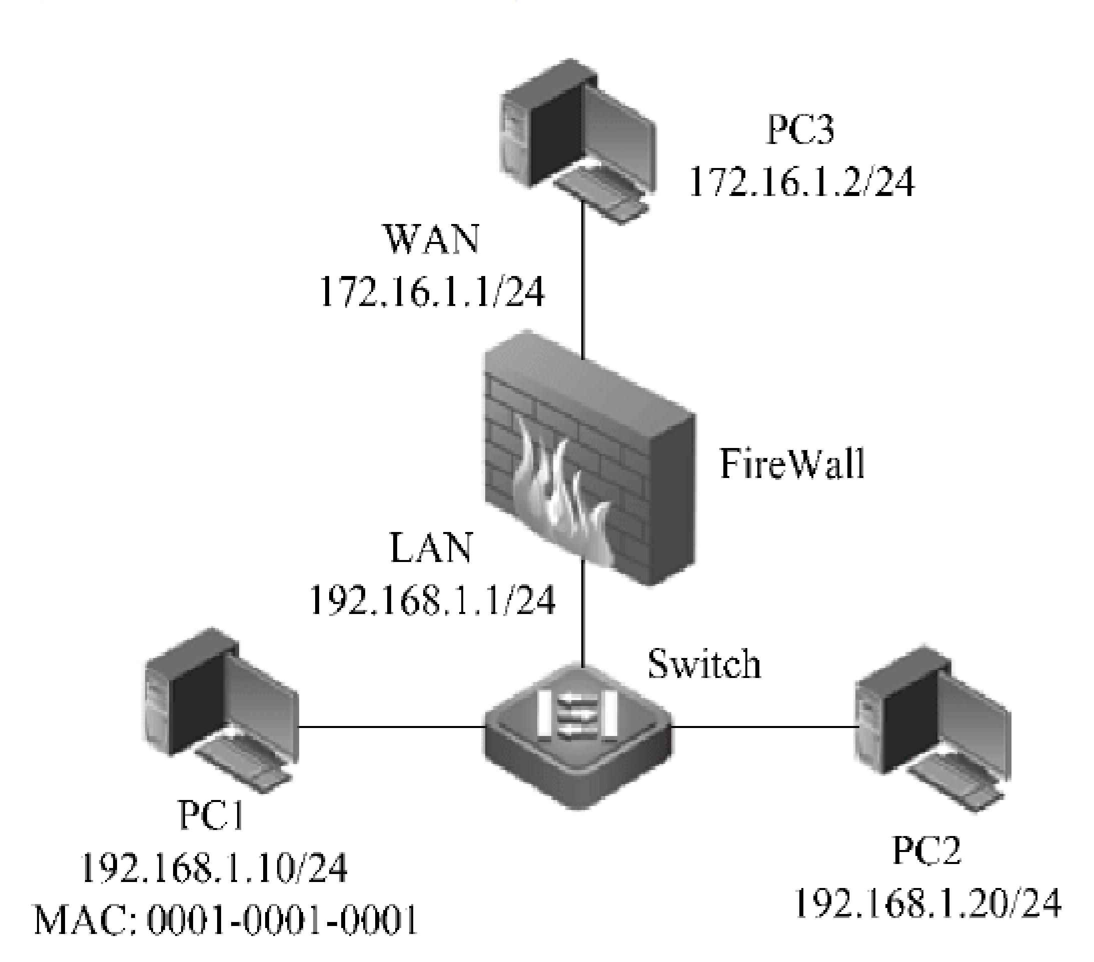



图 2-53　防火墙实现地址绑定网络规划拓扑图

## 【实验设备】

交换机　1 台
防火墙　1 台
PC　　 3 台

## 【预备知识】

- 网络基础知识。
- 防火墙工作原理。

## 【实验原理】

如果防火墙某接口配置了 IP/MAC 端口地址绑定功能，并设置了相应策略（允许或

禁止)，当该接口接收数据包时，防火墙将根据数据包中的源 IP 地址与源 MAC 地址，匹配管理员设置好的 IP/MAC 地址绑定表。如果地址绑定表中查找成功，则按匹配的策略允许或禁止数据包通过，不匹配则禁止数据包通过。如果查找失败，则按默认策略执行。

## 【实验步骤】

### 1. 配置防火墙接口的 IP 地址

如图 2-54 所示，进入防火墙的配置页面，即“网络配置≫接口 IP”页面，单击“添加”按钮，为接口添加 IP 地址。




图 2-54　防火墙的配置页面

为防火墙的 LAN 接口配置 IP 地址及子网掩码，如图 2-55 所示。

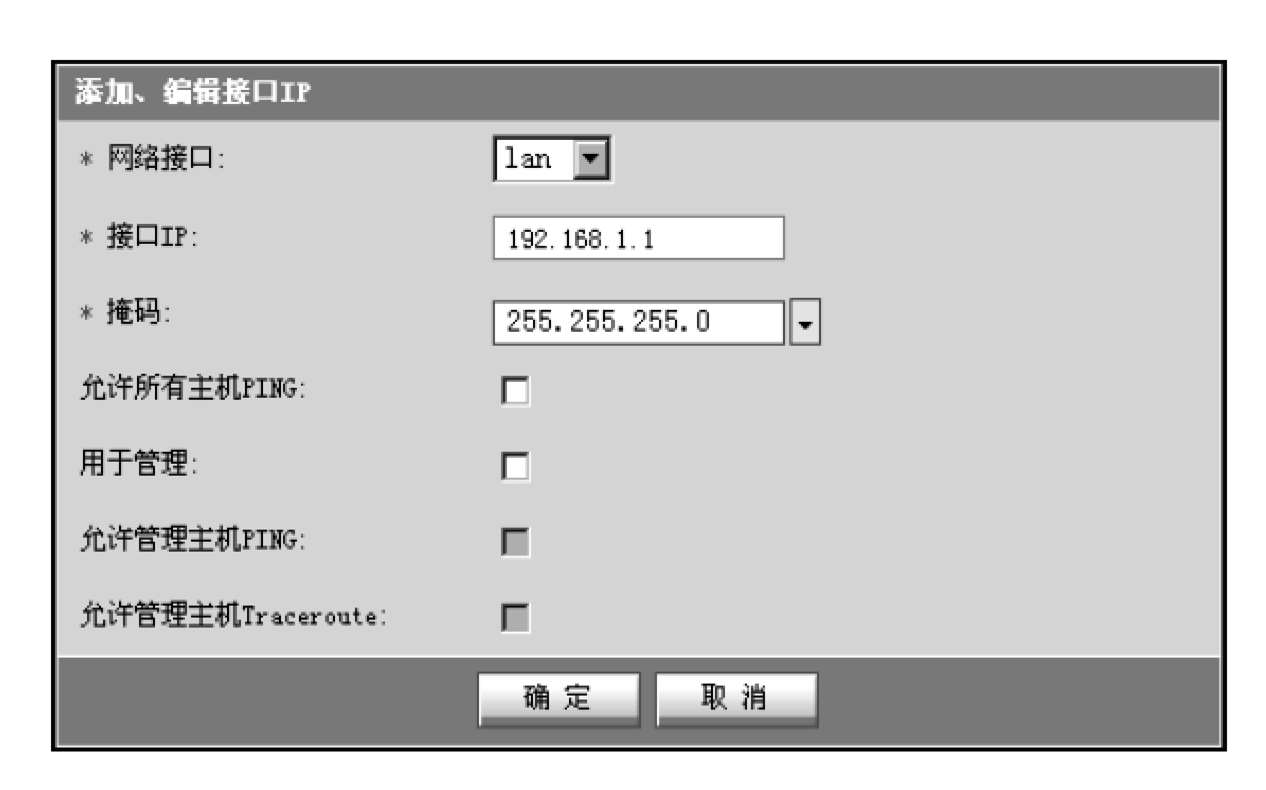



图 2-55　配置防火墙 LAN 接口的 IP 地址

为防火墙的 WAN 接口配置 IP 地址及子网掩码，如图 2-56 所示。

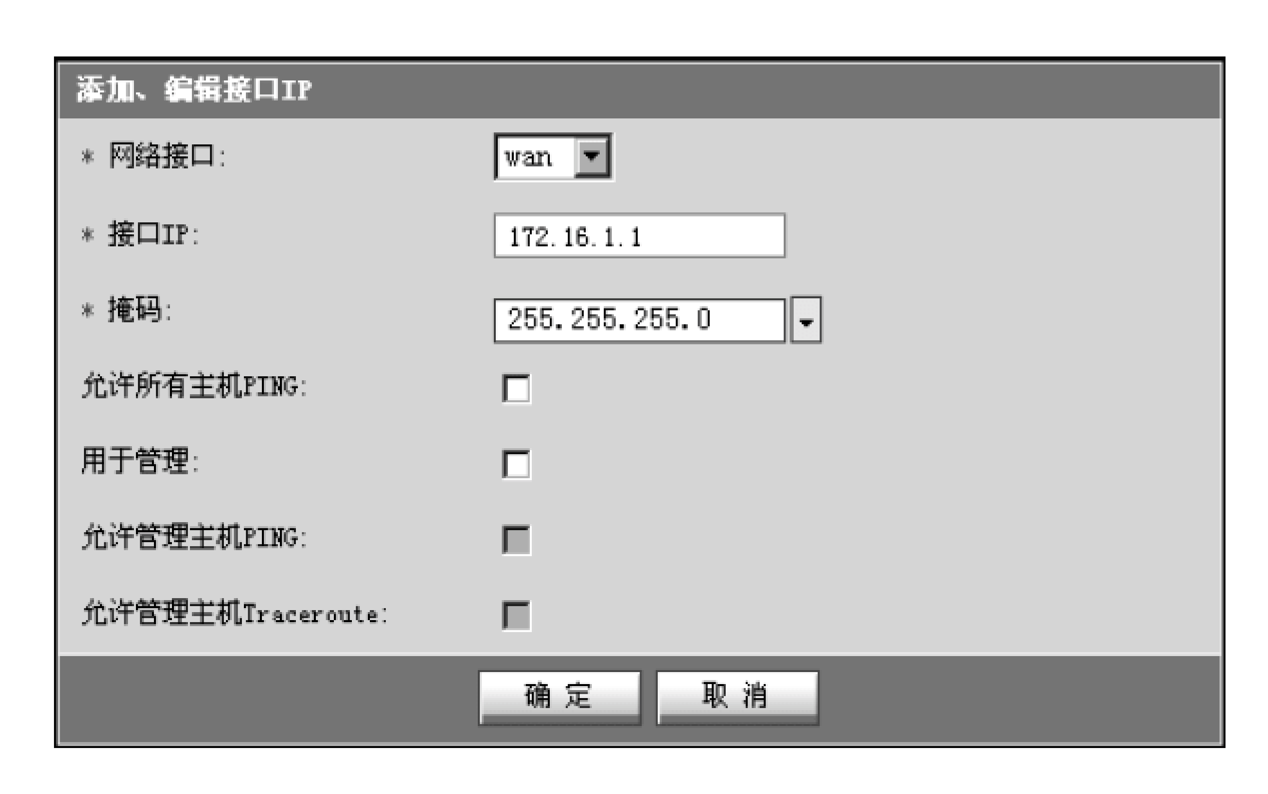



图 2-56　配置防火墙 WAN 接口的 IP 地址

接口配置 IP 地址后的状态如图 2-57 所示。

| 网络接口 | 接口IP | 掩码 | 允许所有主机PING | 用于管理 | 允许管理主机PING | 允许管理主机Traceroute | 操作 |
|---|---|---|---|---|---|---|---|
| ADSL | 未启用 | | | | | | |
| DHCP | 未启用 | | | | | | |
| dmz | 1.1.1.1 | 255.0.0.0 | ✔ | ✔ | ✔ | ✔ | |
| lan | 192.168.1.1 | 255.255.255.0 | ✘ | ✘ | ✘ | ✘ | |
| wan | 172.16.1.1 | 255.255.255.0 | ✘ | ✘ | ✘ | ✘ | |

添 加　刷 新

图 2-57　配置防火墙接口的信息

## 2. 启用 IP/MAC 绑定

进入防火墙配置页面，即“安全策略≫地址绑定”页面，首先启用 LAN 接口的 IP/MAC 绑定功能，并设置默认策略为允许，即如果未查找到 IP/MAC 绑定条目，则允许数据包通过。配置完成后，单击“确定”按钮，如图 2-58 所示。

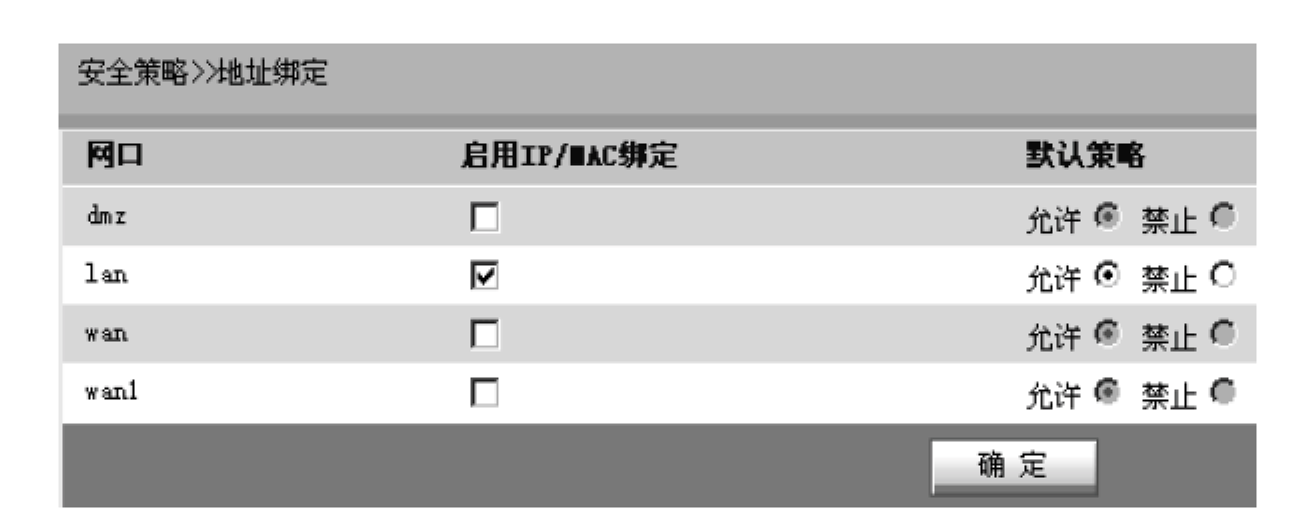



图 2-58　配置防火墙安全策略

## 3. 配置 IP/MAC 地址对

如图 2-59 所示，单击页面上的“添加”按钮，为 PC1 手工添加 IP/MAC 地址来绑定条目(假设 PC1 的 MAC 地址为 00-01-00-01-00-01)，添加结果如图 2-60 所示。




图 2-59　配置防火墙的地址绑定




图 2-60　手工添加 IP/MAC 地址绑定条目

### 4. 配置安全规则

如图 2-42 所示，进入防火墙配置页面，即“安全策略≫安全规则”页面，创建允许 ICMP 的包过滤规则，如图 2-61 所示。




图 2-61 配置防火墙包过滤的安全规则

### 5. 验证测试

- 在 PC1 上执行 ping 172.16.1.2，可以 ping 通。
- 更改 PC1 的地址为 PC2 的地址 192.168.1.20，再次执行 ping 172.16.1.2，则无法 ping 通。因为在防火墙中已经配置了 PC1 的 IP/MAC 绑定，所以防火墙将 PC1（修改 IP 地址后）发送的报文丢弃。

## 2.5 使用防火墙实现 URL 过滤

### 【实验名称】

使用防火墙实现 URL 过滤。

### 【实验目的】

利用防火墙的 URL 过滤功能对用户的 Web 访问进行控制。

### 【背景描述】

某企业网络的出口使用了一台防火墙作为接入 Internet 的设备，并且内部网络使用私有编址方案。最近网络管理员发现，一些员工在上班时间经常访问一些娱乐网站（例如 www.sohu.com），影响了工作质量。

现在公司希望员工在上班时间不能访问这些网站（如 www.sohu.com），但是广告部员工因为业务需要，可以访问这些网站获取信息。

## 【需求分析】

为了限制内部用户访问 Web 站点，可以使用防火墙的 URL 过滤功能，使防火墙阻断内部用户对某些站点（URL）的访问请求。

## 【实验拓扑】

如图 2-62 所示的网络拓扑，企业网络要求限制内部用户访问 Web 站点，使用防火墙的 URL 过滤功能，使防火墙阻断内部用户对某些站点（URL）的访问请求，以实现企业内部网络安全访问控制需求。

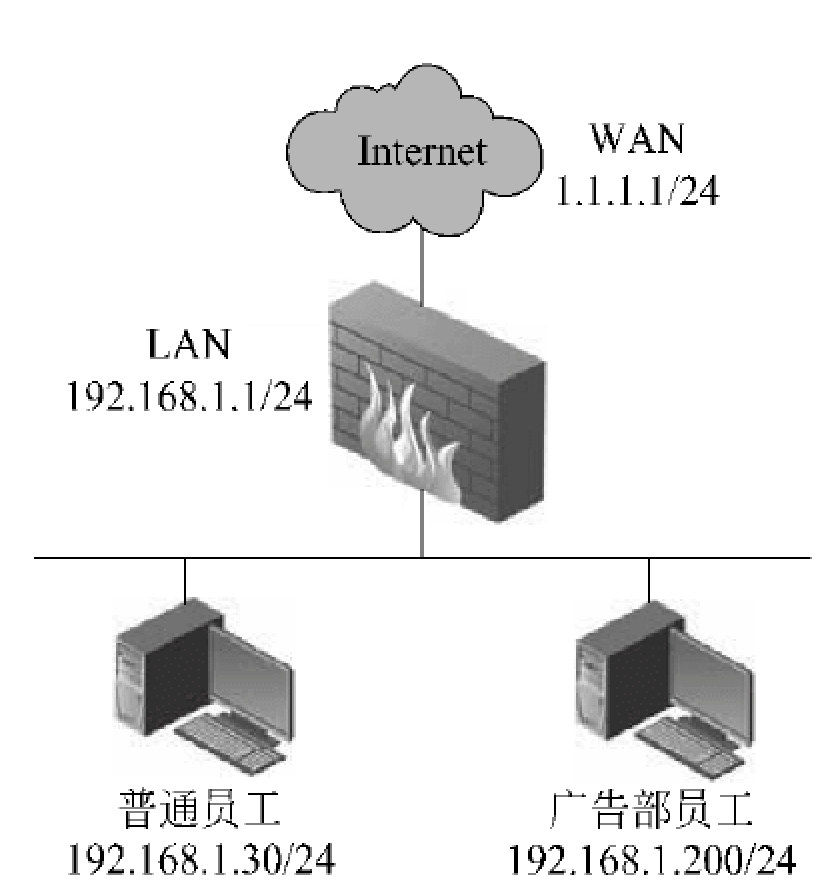



图 2-62　企业网络使用防火墙的 URL 过滤网络规划拓扑图

## 【实验设备】

防火墙连接到 Internet 的链路

防火墙　　1 台

PC　　　　2 台

## 【预备知识】

- 网络基础知识。
- 防火墙的基础知识。

## 【实验原理】

防火墙的 URL 过滤功能可以对用户的 URL 请求进行过滤，只有配置在规则中允许访问的目标 URL 的请求才能够通过防火墙。

## 【实验步骤】

### 1. 配置防火墙接口的 IP 地址

进入防火墙的配置页面，即“网络配置≫接口 IP”页面，单击“添加”按钮，为接口添加 IP 地址。为防火墙的 LAN 接口配置 IP 地址及子网掩码，如图 2-63 所示。

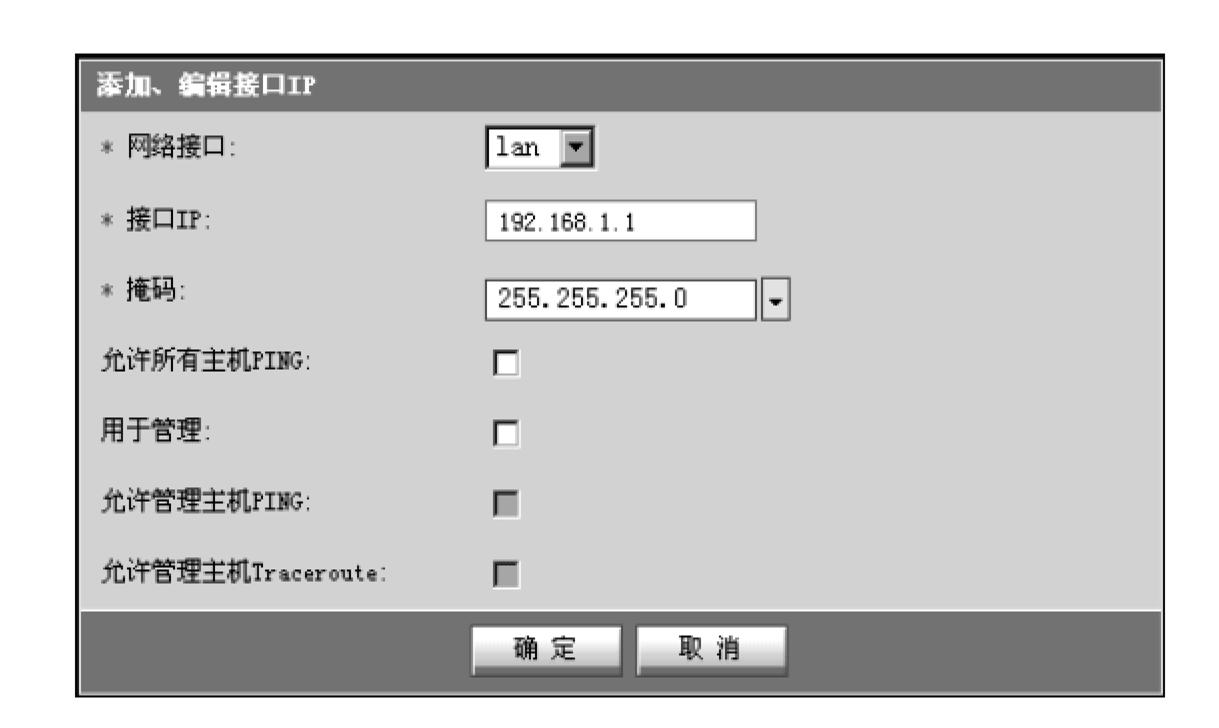



图 2-63　配置防火墙 LAN 接口的 IP 地址

为防火墙的 WAN 接口配置 IP 地址及子网掩码,如图 2-64 所示。

添加、编辑接口IP

* 网络接口: wan

* 接口IP: 1.1.1.1

* 掩码: 255.255.255.0

允许所有主机PING:

用于管理:

允许管理主机PING:

允许管理主机Traceroute:

确 定　取 消

图 2-64　配置防火墙 WAN 接口的 IP 地址

## 2 配置默认路由

进入防火墙的配置页面,即“网络配置≫策略路由”页面,单击“添加”按钮,添加一条浏览 Internet 的默认路由,如图 2-65 所示。




图 2-65　配置防火墙的策略路由

## 3 配置广告部的 NAT 规则

如图 2-42 所示,进入防火墙配置页面,即“安全策略≫安全规则”页面,单击页面上方的“NAT 规则”按钮,添加 NAT 规则,如图 2-66 所示。

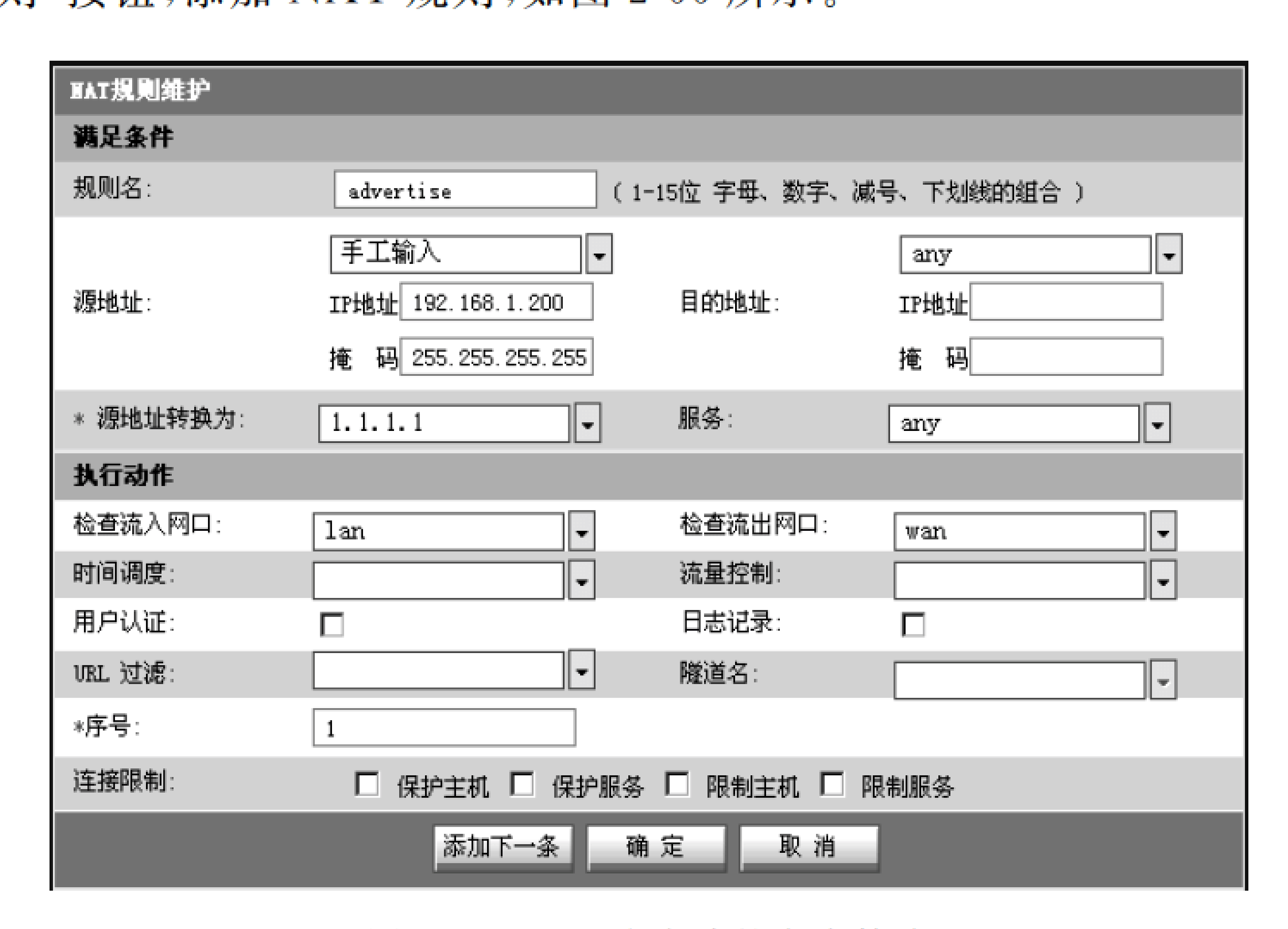



图 2-66　配置防火墙的安全策略

#### 4. 配置 URL 列表

进入防火墙配置页面,即"对象定义≫URL 列表"页面,单击"添加"按钮,创建 URL 列表。

选择 URL 列表的类型为"黑名单",即拒绝访问该 URL;在"http 端口"文本框中输入默认的端口 80;在"添加关键字"文本框中输入 URL 的关键字,如图 2-67 所示。

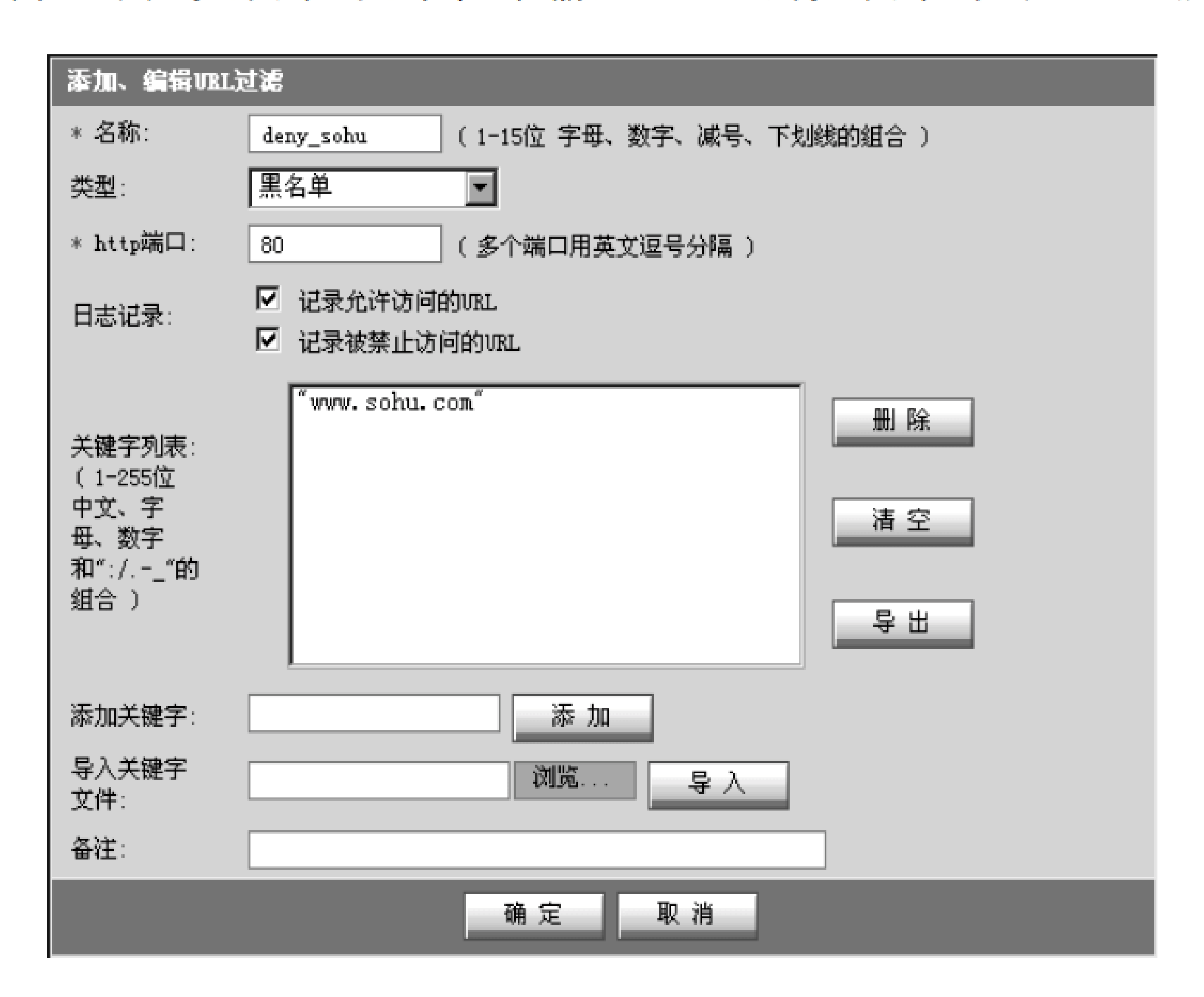



图 2-67　配置防火墙的 URL 列表

#### 5. 配置普通员工的 NAT 规则

进入防火墙配置页面,即"安全策略≫安全规则"页面,单击页面上方的"NAT 规则"按钮,添加 NAT 规则。

在 NAT 规则的"URL 过滤"下拉列表中选择刚才创建的 URL 列表,如图 2-68 所示。




图 2-68　配置防火墙的 NAT 规则

配置完的规则列表如图 2-69 所示。

安全策略>>安全规则　　跳转到 全部

| 序号 | 规则名 | 源地址 | 目的地址 | 服务 | 类型 | 选项 | 生效 |
|---|---|---|---|---|---|---|---|
| ☐ 1 | advertise | 192.168.1.200 | any | any | NAT规则 | | ✔ |
| ☐ 2 | employee | 192.168.1.0 | any | any | NAT规则 | URL | ✔ |

首页　上一页　下一页　尾页　第1页/1页　跳转到 1 页 确定　每页 100 行

图 2-69　配置完防火墙后的规则列表

## 6. 验证测试

在广告部的 PC 上使用浏览器访问 www. sohu. com，可以成功访问该网站，如图 2-70 所示。




图 2-70　验证测试(1)

在普通员工的 PC 上使用浏览器访问 www. sohu. com，将无法打开该网页，因为防火墙已经阻断访问 www. sohu. com 的请求，如图 2-71 所示。

## 【注意事项】

- 防火墙的 NAT 规则是按照顺序进行匹配的，如果数据流匹配到某条规则后，将不再进行后续规则的匹配。所以需要将广告部的 NAT 规则放置在其他用户的 NAT 规则的前面。
- 在本实验中防火墙 WAN 接口使用的地址为虚拟的，请根据实际网络情况配置正确的公网地址和默认路由的下一跳地址。

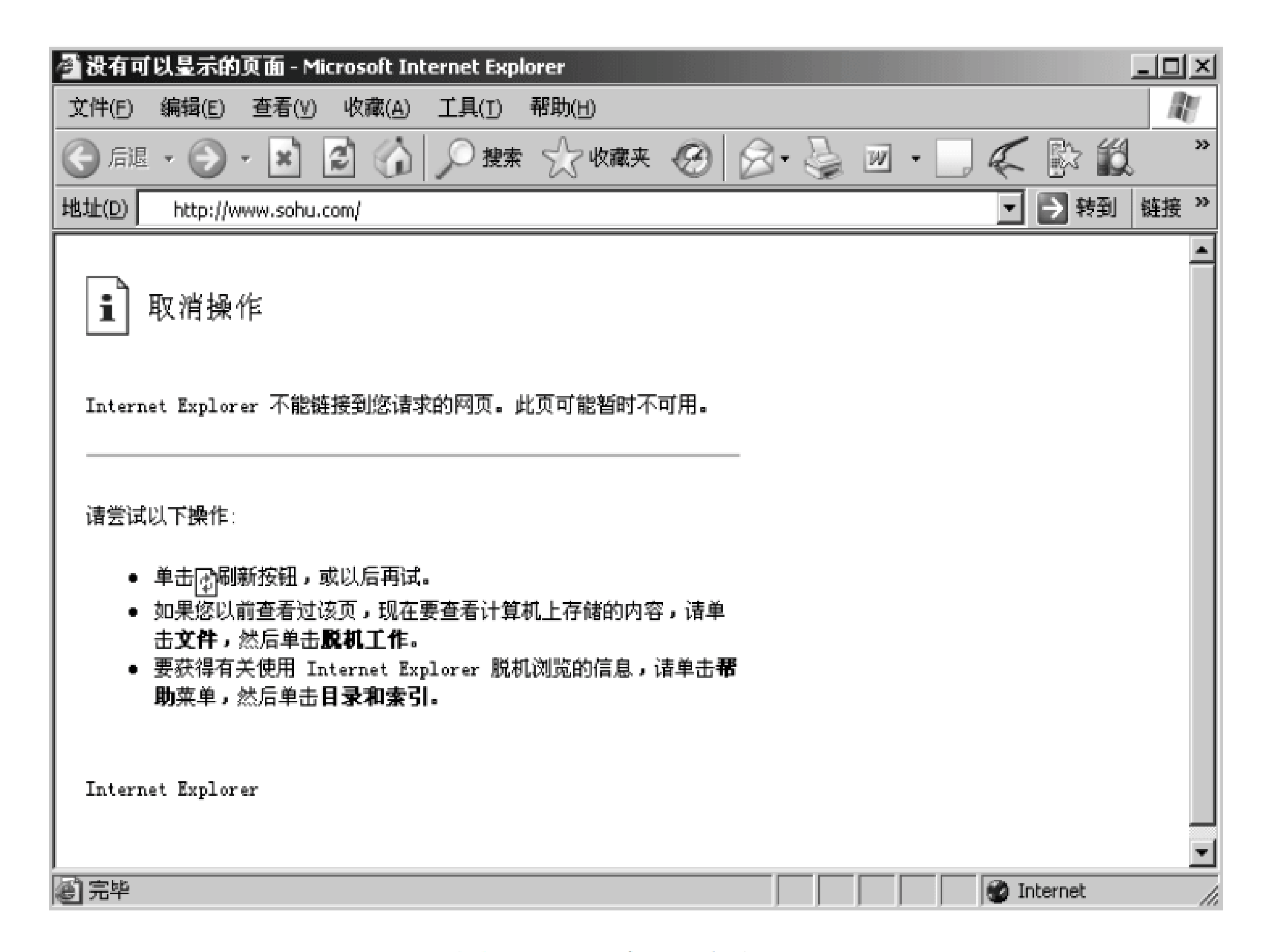



图 2-71　验证测试(2)

# 2.6 使用防火墙保护服务资源

## 【实验名称】

使用防火墙保护服务资源。

## 【实验目的】

利用防火墙保护服务器的资源。

## 【背景描述】

某公司使用防火墙作为网络出口设备，并且在防火墙的 DMZ 区域中部署一台提供对外服务的 Web 服务器。但网络管理员经常发现有大量浏览服务器的连接，致使消耗了服务器的大量系统资源，使其不能提供良好的服务。为了使 Web 服务器正常提供服务，需要保护服务器的系统资源，限制浏览服务器的连接数。

## 【需求分析】

通过控制浏览服务器的连接数，从而保护服务器的系统资源，使服务器正常提供服务。防火墙的服务保护功能可以对浏览服务器的连接数量进行限制。

## 【实验拓扑】

如图 2-72 所示的网络拓扑，企业网络为了使 Web 服务器正常提供服务，保护服务器

的系统资源,通过限制浏览服务器的连接数,以实现企业内部网络安全访问控制需求。

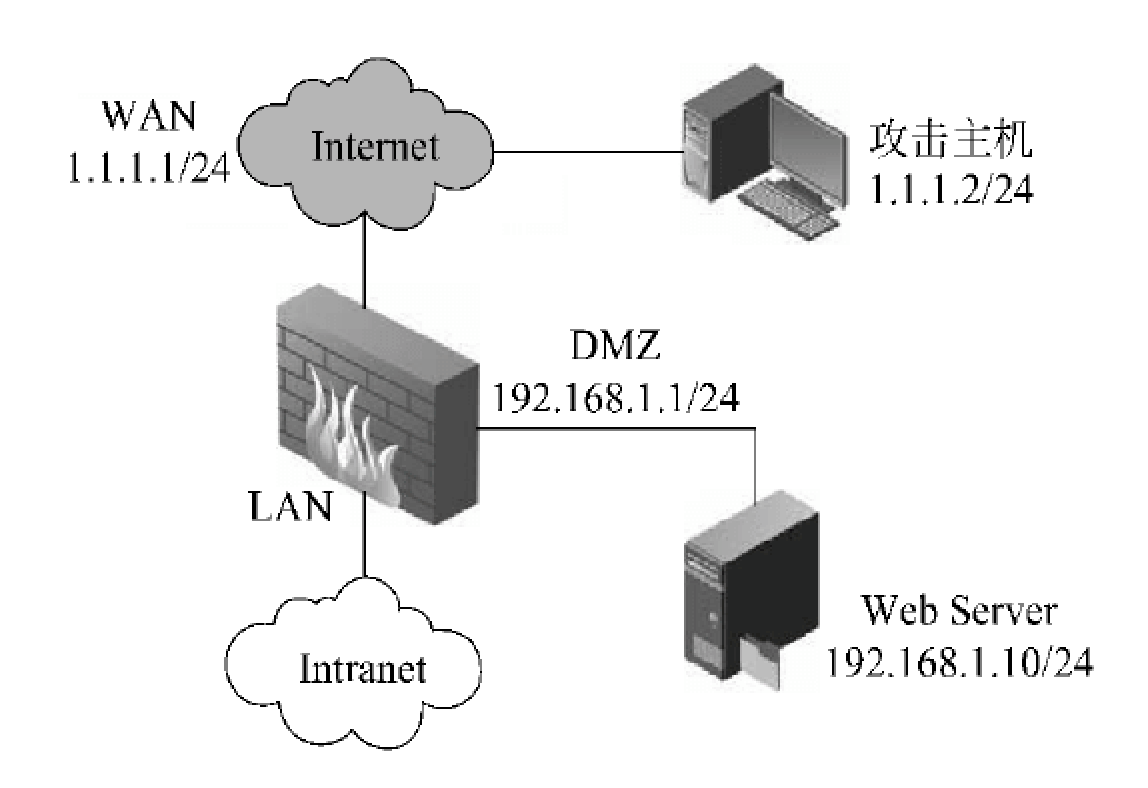



图 2-72　防火墙限制服务器连接数网络规划拓扑图

## 【实验设备】

防火墙　　1 台

PC　　2 台(一台作为 Web 服务器;另一台模拟外部网络的攻击主机)

Web 服务器软件程序　　TCP 攻击软件程序

## 【预备知识】

- 网络基础知识。
- 防火墙工作原理。

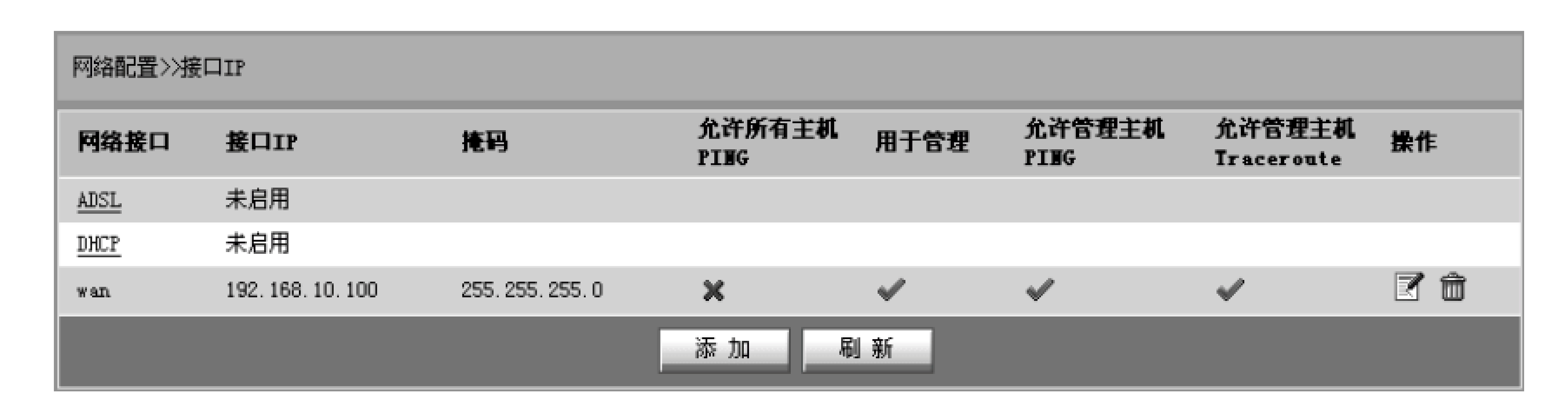
## 【实验原理】

服务保护是防火墙的一种安全功能,可以限制从某个区域到达另外一个区域中主机或服务器的连接数。

## 【实验步骤】

### 1. 配置防火墙接口的 IP 地址

如图 2-73 所示,进入防火墙的配置页面,即“网络配置≫接口 IP”页面,单击“添加”按钮,为接口添加 IP 地址。



网络配置>>接口IP

| 网络接口 | 接口IP | 掩码 | 允许所有主机PING | 用于管理 | 允许管理主机PING | 允许管理主机Traceroute | 操作 |
| --- | --- | --- | --- | --- | --- | --- | --- |
| ADSL | 未启用 | | | | | | |
| DHCP | 未启用 | | | | | | |
| wan | 192.168.10.100 | 255.255.255.0 | ✕ | ✔ | ✔ | ✔ | |

添 加　刷 新

图 2-73　配置防火墙接口的 IP 地址

为防火墙的 DMZ 接口配置 IP 地址及子网掩码，如图 2-74 所示。

添加、编辑接口IP
* 网络接口: dmz
* 接口IP: 192.168.1.1
* 掩码: 255.255.255.0
允许所有主机PING:
用于管理:
允许管理主机PING:
允许管理主机Traceroute:
确 定 取 消

图 2-74　配置防火墙 DMZ 接口的 IP 地址

为防火墙的 WAN 接口配置 IP 地址及子网掩码，如图 2-75 所示。

添加、编辑接口IP
* 网络接口: wan
* 接口IP: 1.1.1.1
* 掩码: 255.255.255.0
允许所有主机PING:
用于管理:
允许管理主机PING:
允许管理主机Traceroute:
确 定 取 消

图 2-75　配置防火墙 WAN 接口的 IP 地址

### 2 配置端口映射规则

为了使 Internet 中的用户可以访问 DMZ 中的 Web 服务器，需要在防火墙上使用端口映射规则，将 Web 服务器发布到 Internet 中。

进入防火墙配置页面，即“安全策略≫安全规则”页面，单击页面上方的“端口映射规则”按钮，添加端口映射规则。规则中的“公开地址”为防火墙外部接口（WAN）的地址；“内部地址”为 DMZ 中的 Web 服务器的地址；“内部服务”为 Web 服务器提供 Web 服务使用的端口号，这里使用默认的 80 端口（HTTP）；“对外服务”为 Internet 用户访问 Web 服务器时使用的在外部看到的端口号，这里也使用默认的 80 端口（HTTP），如图 2-76 所示。

### 3 验证测试

在 DMZ 中的 PC 上安装好 Web Server 程序，并进行相应的配置。在外部 PC 上测试浏览 Web 服务器的连通性，注意这里使用的目标地址为 1.1.1.1。防火墙将其发送到 1.1.1.1，端口为 80 的请求重定向到 DMZ 中的 Web 服务器，如图 2-77 所示。

| 端口映射规则维护 | | | |
|---|---|---|---|
| **满足条件** | | | |
| 规则名: | pnat1 （1-15位 字母、数字、减号、下划线的组合） | | |
| 源地址: | IP地址　掩　码 | * 公开地址: | 1.1.1.1 |
| 源地址转换为: | | * 内部地址: | 手工输入　IP地址 192.168.1.10 |
| * 对外服务: | http | * 内部服务: | http |
| **执行动作** | | | |
| 检查流入网口: | wan | 检查流出网口: | dmz |
| 时间调度: | | 流量控制: | |
| 用户认证: | ☐ | 日志记录: | ☐ |
| 隧道名: | | 序号: | 1 |
| 连接限制: | ☐ 保护主机 ☐ 保护服务 ☐ 限制主机 ☐ 限制服务 | | |
| | 添加下一条　确 定　取 消 | | |

图 2-76　配置防火墙的端口映射规则

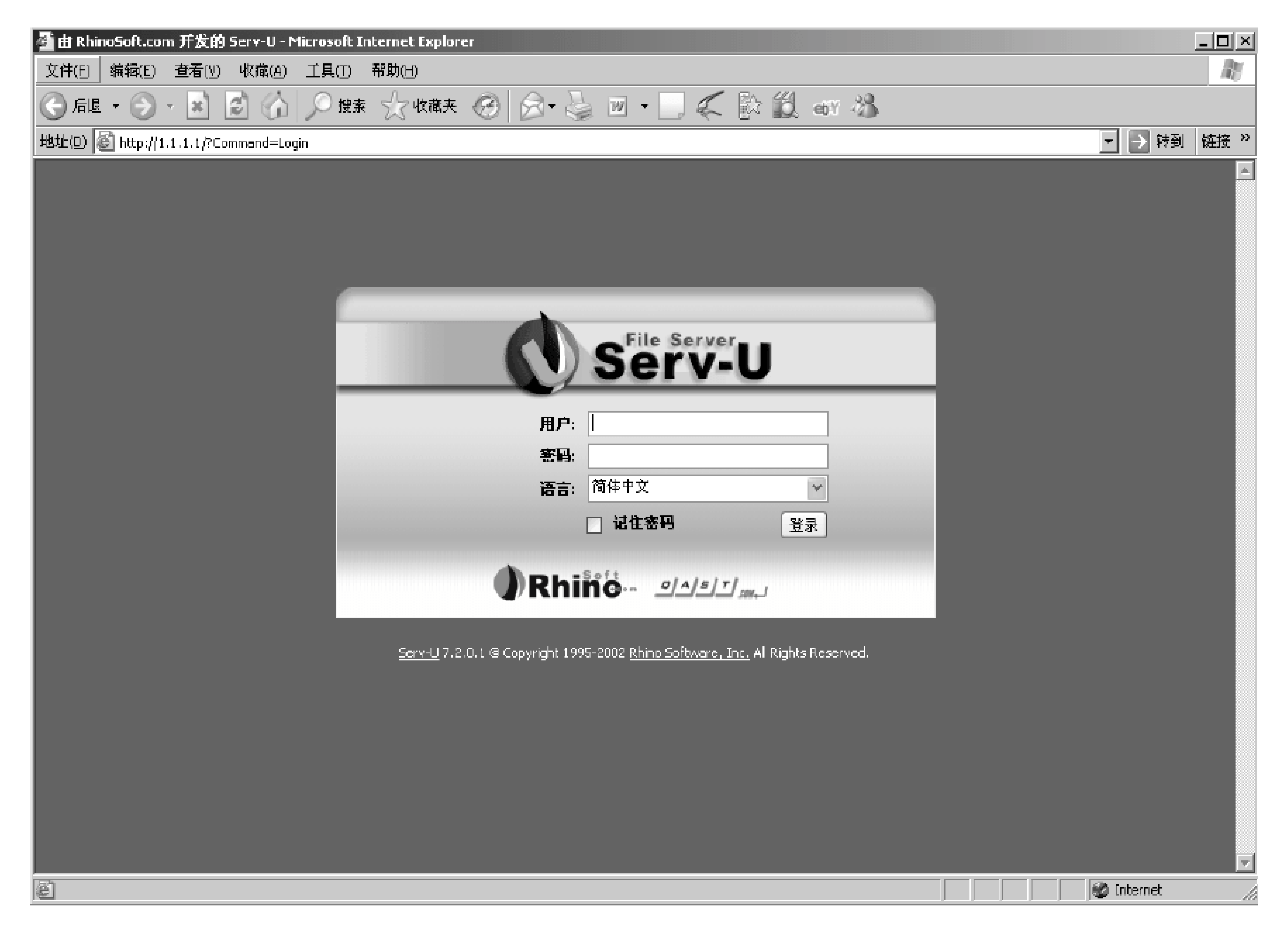



图 2-77　外部 PC 测试浏览服务器的连通性

外部 PC 可以通过预先设置的用户名和密码登录到 Web 服务器,如图 2-78 所示。

### 4. 实施 TCP 攻击

在外部 PC 上使用 TCP 连接工具向 Web 服务器发起攻击,建立大量的 TCP 连接。此时在 Web 服务器上通过 Windows 命令 netstat -an 可以看到外部主机与 Web 服务器的 http 端口建立了大量的 TCP 连接,状态为 ESTABLISHED,如图 2-79 所示。

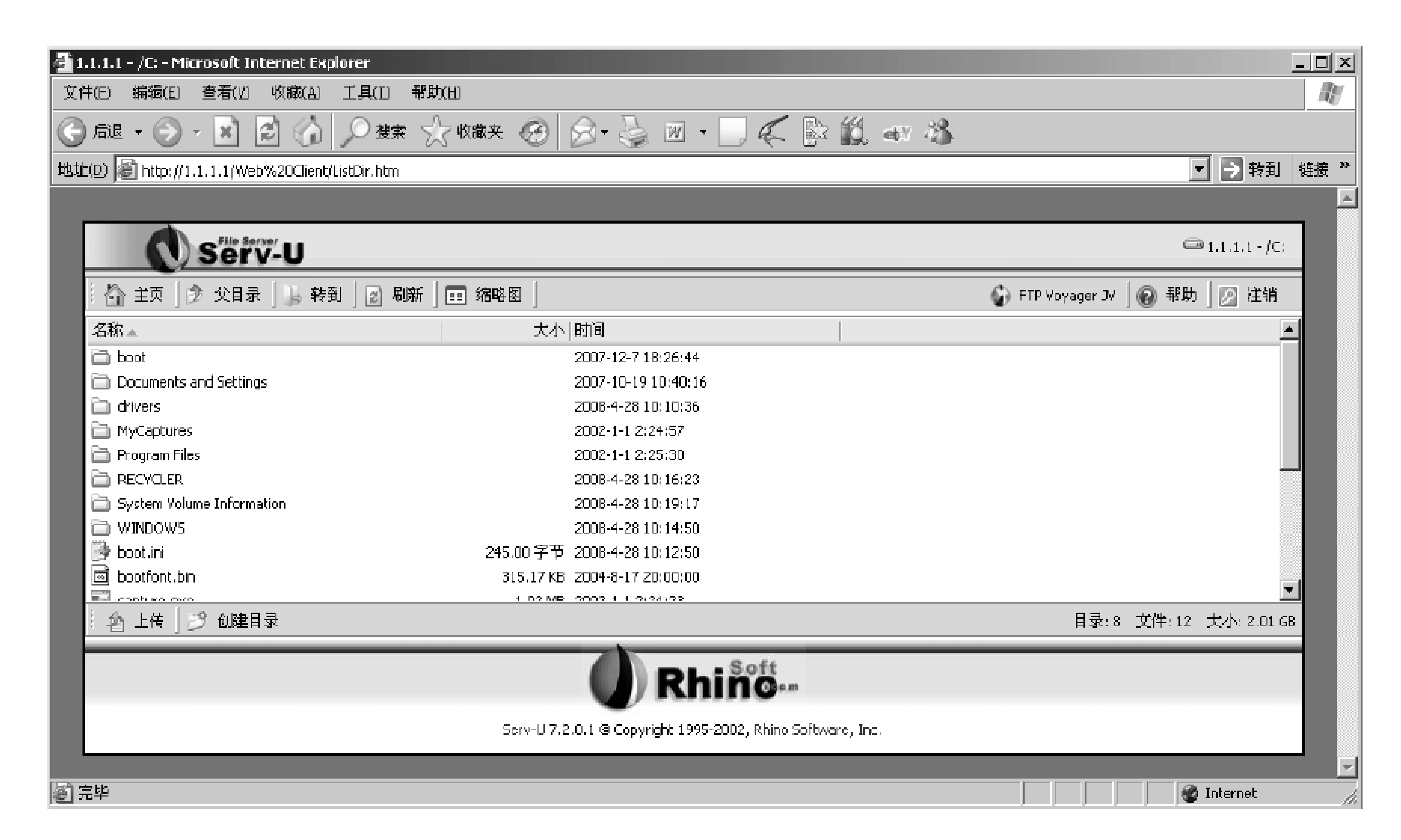



图 2-78 登录 Web 服务器

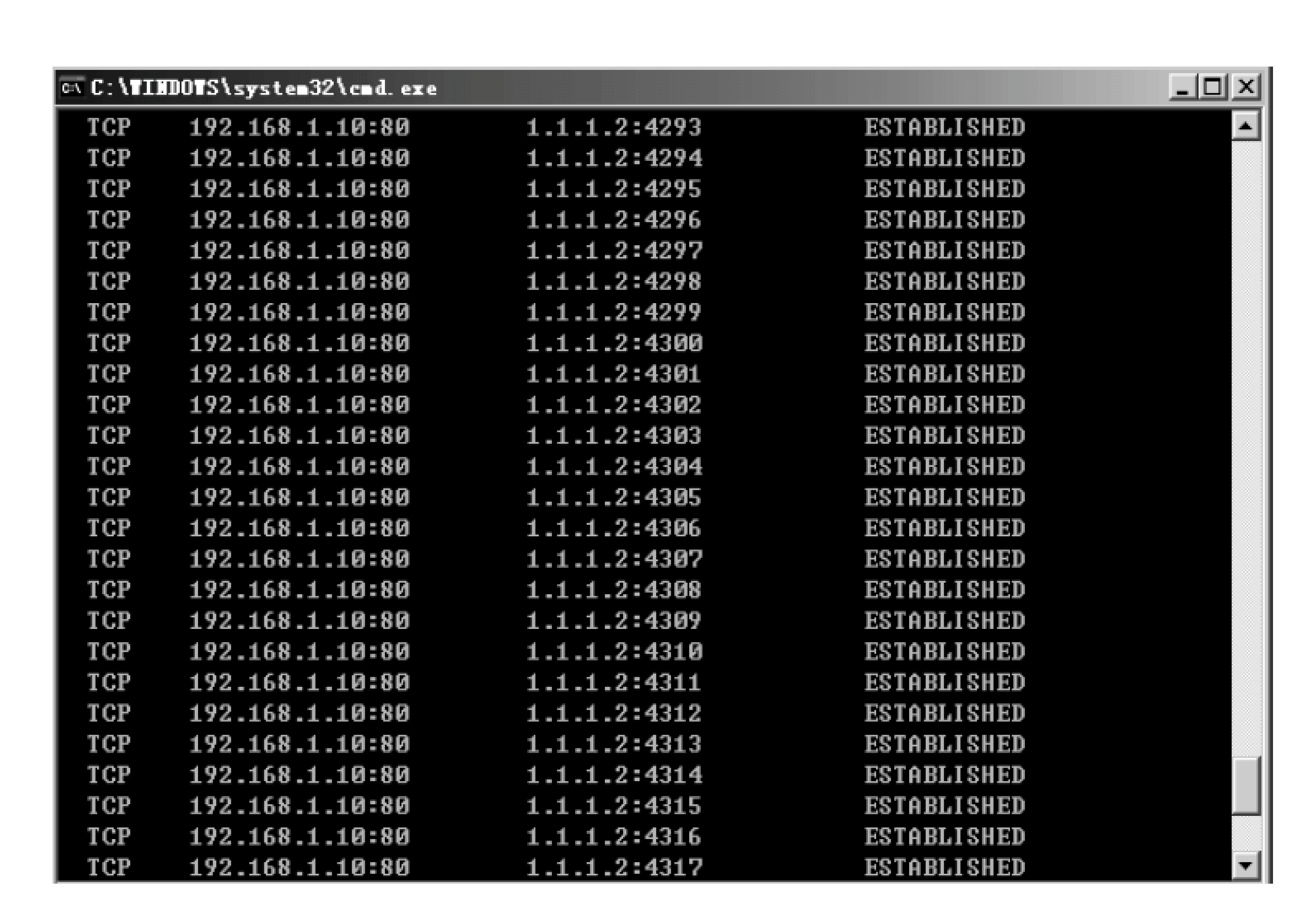



图 2-79 使用 TCP 连接工具向 Web 服务器发起攻击

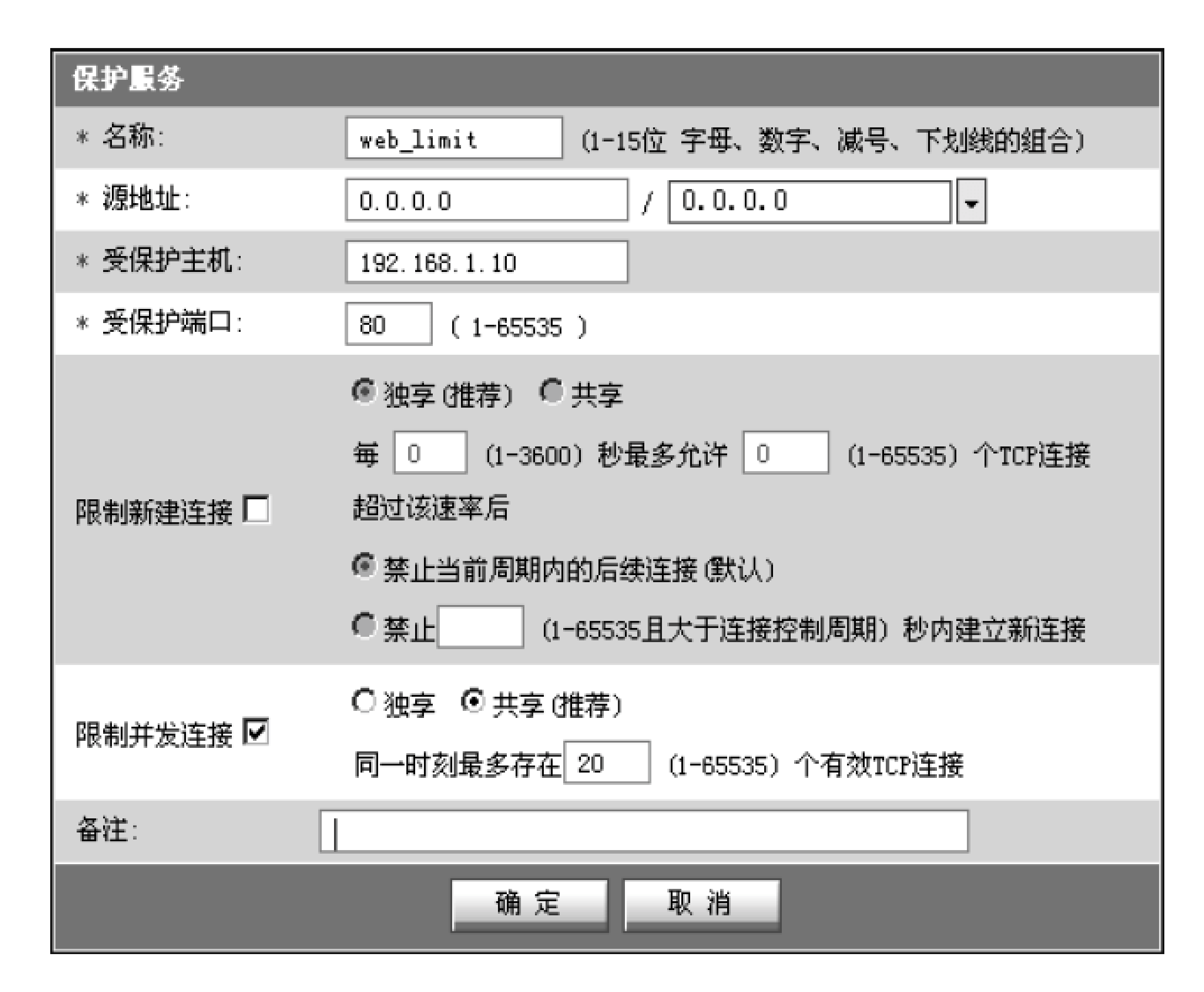
### 5. 配置服务保护规则

进入防火墙配置页面，即“对象定义≫连接限制≫保护服务”页面，单击“添加”按钮，创建规则。

在服务保护规则中，源地址使用 0.0.0.0/0，即代表所有发起连接的源地址；受保护主机为 DMZ 中的 Web 服务器；受保护端口为 Web 服务器的端口 80；最后勾选“限制并发连接”复选框，将同一时刻最多存在的有效 TCP 连接数设置为 20，如图 2-80 所示。

### 6. 应用服务保护规则

进入防火墙配置页面，即“安全策略≫安全规则”页面，对之前创建的端口映射规则进行编辑。在该规则中勾选“保护服务”复选框，如图 2-81 所示。


保护服务

| | |
|---|---|
| * 名称: | web_limit （1-15位 字母、数字、减号、下划线的组合） |
| * 源地址: | 0.0.0.0 / 0.0.0.0 |
| * 受保护主机: | 192.168.1.10 |
| * 受保护端口: | 80 （1-65535 ） |
| 限制新建连接 ☐ | ◉ 独享（推荐） ○ 共享<br>每 0 （1-3600）秒最多允许 0 （1-65535）个TCP连接<br>超过该速率后<br>◉ 禁止当前周期内的后续连接（默认）<br>○ 禁止 （1-65535且大于连接控制周期）秒内建立新连接 |
| 限制并发连接 ☑ | ○ 独享 ◉ 共享（推荐）<br>同一时刻最多存在 20 （1-65535）个有效TCP连接 |
| 备注: | |

确 定　取 消

图 2-80　配置防火墙的服务保护规则

端口映射规则维护

满足条件

| | | | |
|---|---|---|---|
| 规则名: | pnat1 （1-15位 字母、数字、减号、下划线的组合 ） | | |
| 源地址: | 手工输入<br>IP地址 0.0.0.0<br>掩　码 0.0.0.0 | * 公开地址: | 1.1.1.1 |
| 源地址转换为: | 不转换 | * 内部地址: | 手工输入<br>IP地址 192.168.1.10 |
| * 对外服务: | http | * 内部服务: | http |

执行动作

| | | | |
|---|---|---|---|
| 检查流入网口: | wan | 检查流出网口: | dmz |
| 时间调度: | 无 | 流量控制: | 无 |
| 用户认证: | ☐ | 日志记录: | ☐ |
| 隧道名: | 无 | 序号: | 1 |
| 连接限制: | ☐ 保护主机 ☑ 保护服务 ☐ 限制主机 ☐ 限制服务 | | |

确 定　取 消

图 2-81　应用服务保护规则

### 7. 验证测试

在外部 PC 上使用 TCP 连接工具再次向 Web 服务器发起大量攻击。此时在 Web 服务器上通过 Windows 命令 netstat -an 可以看到外部主机与 Web 服务器的 80 端口只建立 20 个 TCP 连接,其他所有的连接建立请求已经被防火墙阻断,如图 2-82 所示。

## 【注意事项】

TCP 连接数量不要设置得过小,这样可能导致合法的连接请求无法建立。

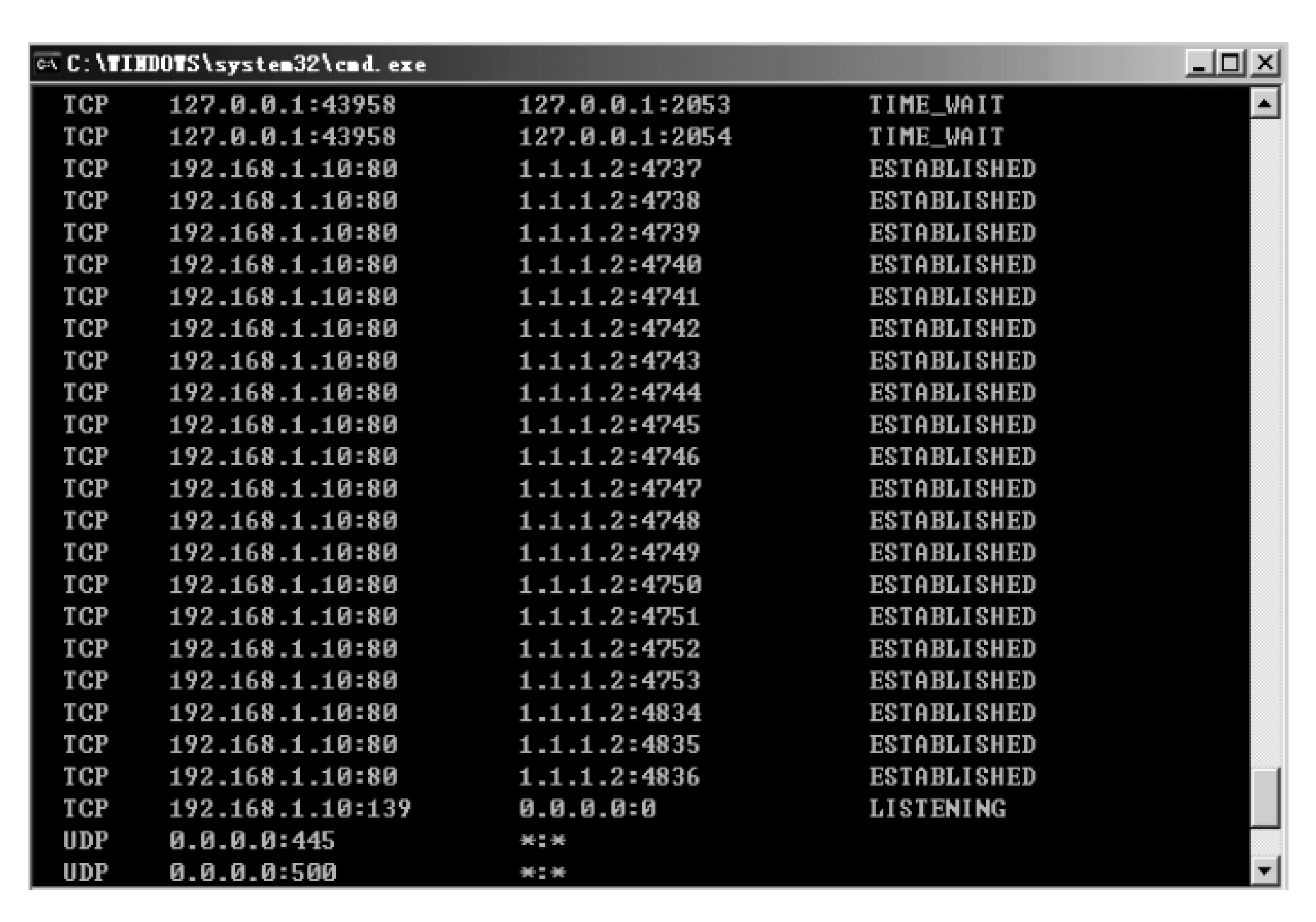



图 2-82　应用服务保护规则验证测试

## 2.7　配置客户端认证

### 【实验名称】

配置客户端认证。

### 【实验目的】

使用防火墙的客户端认证功能来增强访问控制的安全性。

### 【背景描述】

某企业使用防火墙作为网络出口设备。公司内部使用私有编址方案，因此在防火墙上配置了 NAT 规则以使内部用户可以访问 Internet。但是为了避免非授权用户使用公司带宽资源来访问 Internet，需要对客户端进行身份验证，只有通过身份验证的用户才能访问 Internet。此外，管理员不需要进行身份验证。

### 【需求分析】

为了使非授权用户无法通过防火墙访问 Internet，可以利用防火墙对客户端进行认证，只有通过身份验证的用户才能访问 Internet。

### 【实验拓扑】

如图 2-83 所示的网络拓扑，企业网络为了使非授权用户无法通过防火墙访问 Internet，利用防火墙对客户端进行认证，只有通过身份验证的用户才能访问 Internet，以实现企业内部网络安全访问控制需求。

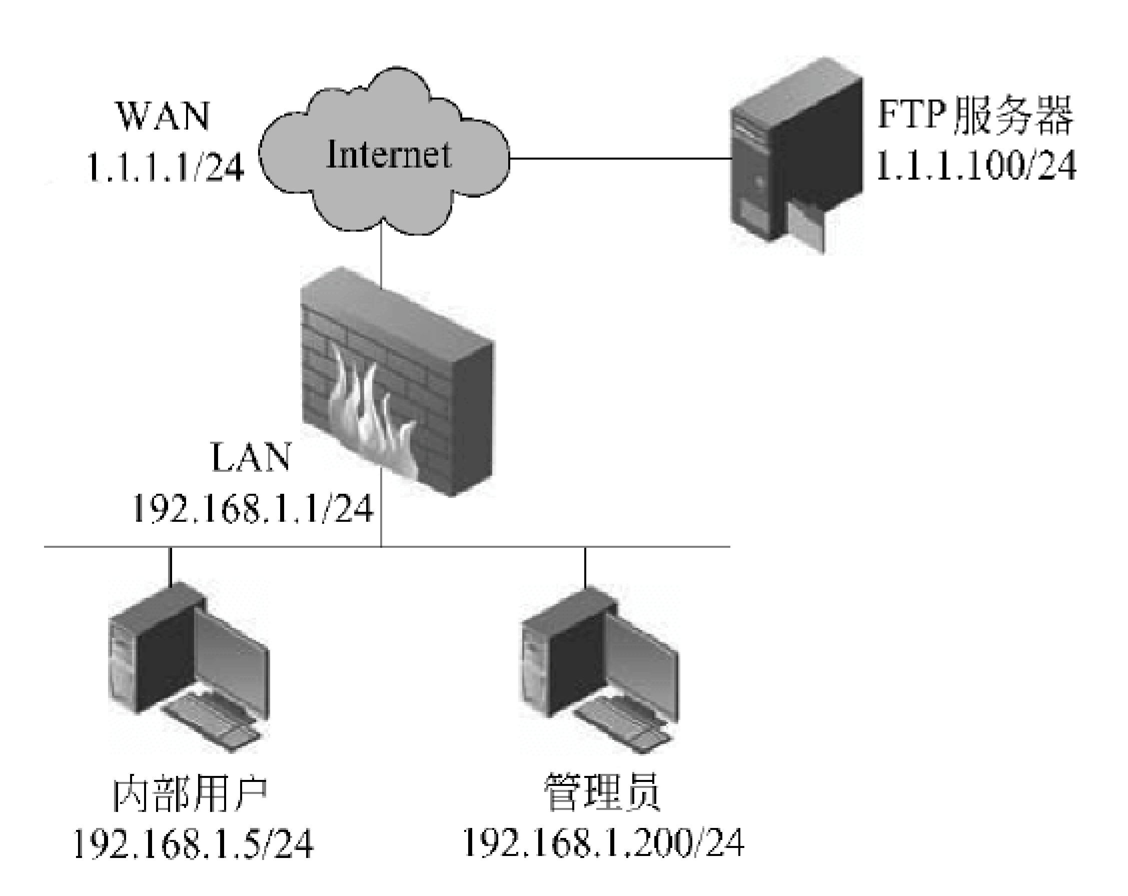



图 2-83　防火墙对客户端进行认证网络规划拓扑图

## 【实验设备】

| | |
|---|---|
| 防火墙 | 1 台 |
| PC | 3 台(其中一台模拟 Internet 的 FTP 服务器) |
| FTP 服务器软件程序 | 防火墙客户端认证程序 |

## 【预备知识】

- 网络基础知识。
- 防火墙工作原理。

## 【实验原理】

RG-WALL 防火墙的访问控制功能可以对客户端的身份进行验证,只有客户端通过验证后,才允许通过安全策略来访问网络资源。

## 【实验步骤】

### 1. 配置防火墙接口的 IP 地址

进入防火墙的配置页面,即“网络配置≫接口 IP”页面,单击“添加”按钮,为接口添加 IP 地址。为防火墙的 LAN 接口配置 IP 地址及子网掩码,如图 2-84 所示。

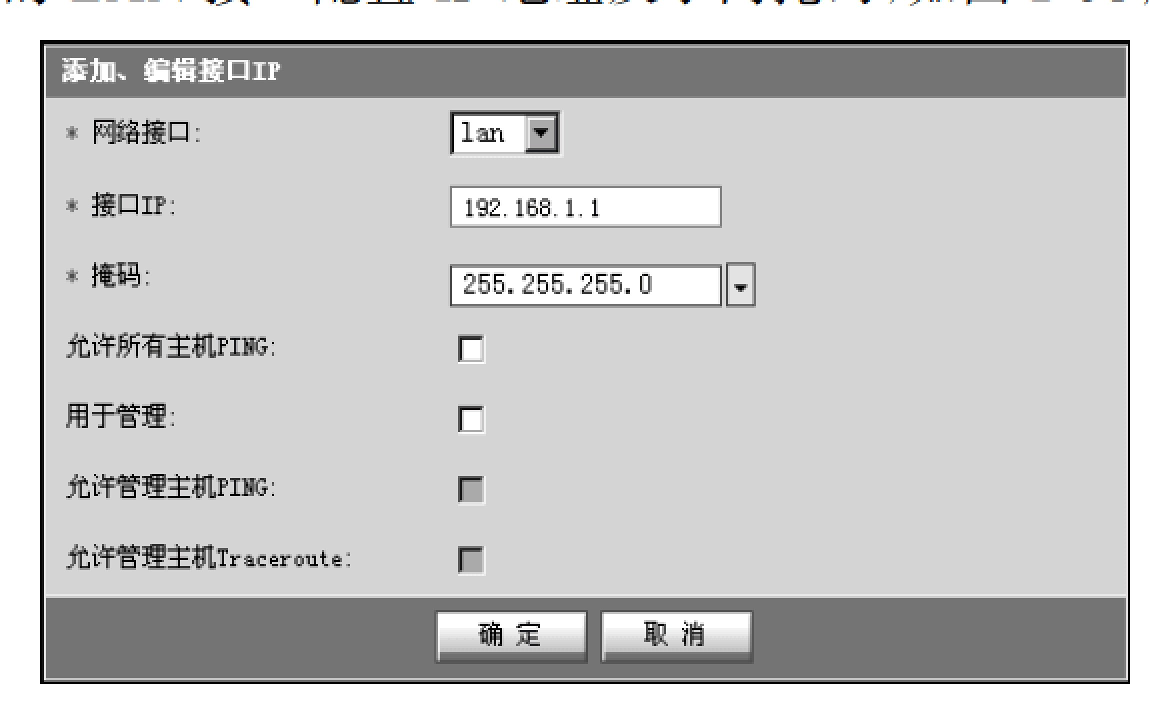



图 2-84　配置防火墙 LAN 接口的 IP 地址

为防火墙的 WAN 接口配置 IP 地址及子网掩码，如图 2-85 所示。

图 2-85 配置防火墙 WAN 接口的 IP 地址

## 2. 配置管理员的 NAT 规则

如图 2-42 所示，进入防火墙配置页面，即“安全策略≫安全规则”页面，单击页面上方的“NAT 规则”按钮，添加 NAT 规则，即可启动 NAT 规则配置页面，如图 2-86 所示。

图 2-86 配置管理员的 NAT 规则

## 3. 配置内部用户的 NAT 规则

进入防火墙配置页面，即“安全策略≫安全规则”页面，单击页面上方的“NAT 规则”按钮，添加 NAT 规则。

在内部用户的 NAT 规则中，需要勾选“用户认证”复选框，这样防火墙将对内部用户进行身份验证，如图 2-87 所示。

配置完 NAT 规则后的规则列表如图 2-88 所示。

## 4. 验证测试

在管理员 PC 上访问外部的 FTP 服务器 1.1.1.100，可以成功访问，因为管理员的 NAT 规则中没有要求进行用户认证，如图 2-89 所示。




图 2-87 配置内部用户的 NAT 规则

安全策略>>安全规则　　跳转到 全部

| 序号 | 规则名 | 源地址 | 目的地址 | 服务 | 类型 | 选项 | 生效 |
|---|---|---|---|---|---|---|---|
| 1 | nat1 | 192.168.1.200 | any | any | NAT规则 | | ✔ |
| 2 | nat2 | 192.168.1.0 | any | any | NAT规则 | | ✔ |

首页 上一页 下一页 尾页 第1页/1页 跳转到 1 页 确定 每页 100 行

图 2-88 完成防火墙配置后的 NAT 规则列表




图 2-89 配置防火墙验证测试

在内部用户 PC 上访问外部的 FTP 服务器 1.1.1.100，访问不成功，因为内部用户的 NAT 规则中要求进行用户认证，如图 2-90 所示。

## 5. 配置用户组

进入防火墙配置页面，即"用户认证≫用户组"页面，单击"添加"按钮，添加用户组。

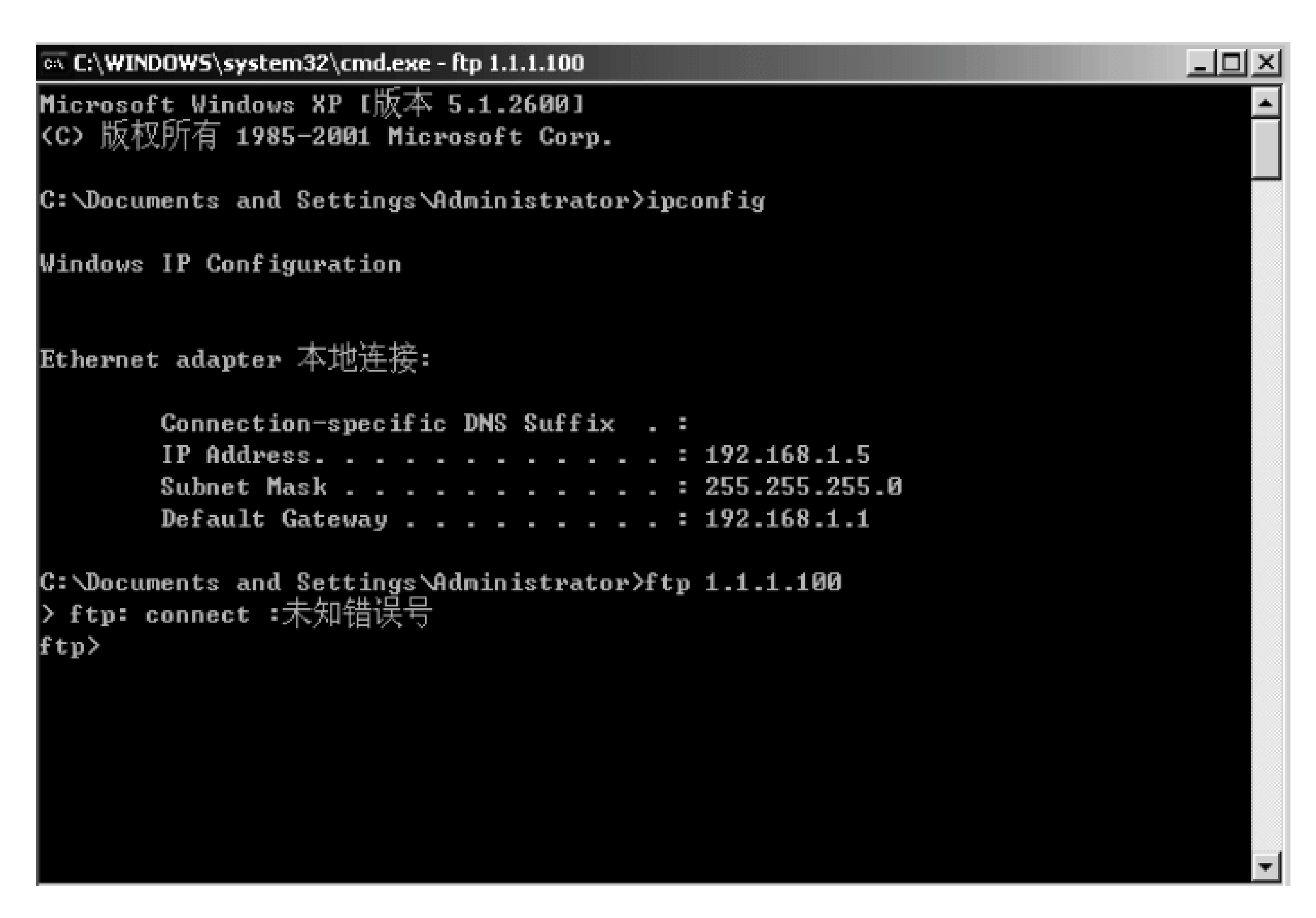



图 2-90　防火墙 NAT 规则验证测试

用户组的认证协议使用“PAP”方式，并确认已勾选“启用本组账号”复选框。

在“安全策略表”区域中单击“添加”按钮，设置允许该组用户从哪些地址和什么时间进行登录，这里我们选择所有地址(any)和任何时间(无)。

在“可使用服务列表”区域中单击“添加”按钮，设置允许该组用户访问哪些地址、服务和什么时间可以访问，这里我们选择所有地址(any)、所有服务(any)和任何时间(无)，如图 2-91 所示。

添加、编辑用户组
* 名称: inside_user (1-15位 字母、数字、减号、下划线的组合)
认证协议: PAP
分配流量: 0 (KB 千字节 范围: 0-4194304, 0表示无限制)
分配时间: 0 (分钟 范围: 0-65535, 0表示无限制)
账号有效期至: 2008 年 12 月 30 日
密码修改最长间隔: 0 (天 范围: 0-999, 0表示无限制)
启用本组账号: ☑
自动重置: ☐ 每月 01 日 每周 一
本组用户: 所有用户 操作 本组用户 >> <<
安全策略表: 允许登录地址 any 时间调度 无 添 加
可使用服务列表: 可连接目的地址 any 可使用服务 any 时间调度 无 添 加
备注:

图 2-91　配置防火墙的用户组

## 6. 配置用户

进入防火墙配置页面，即“用户认证≫用户列表”页面，单击“添加”按钮，添加用户。

输入用户名和密码，将用户加入到之前创建的用户组中，并确认已勾选“启用本账号”复选框，如图 2-92 所示。




图 2-92　配置用户

## 7. 配置安全规则

为了使客户端能够认证成功，需要添加一条安全规则，即允许内部用户访问防火墙的认证流量。

进入防火墙配置页面，即“安全策略≫安全规则”页面，单击“包过滤规则”按钮，添加包过滤规则。规则中的源地址为 192.168.1.0/24；目的地址为防火墙 LAN 接口的地址；在“服务”下拉列表中选择“firewall_auth”，这是客户端认证流量使用的端口号；在“检查流入网口”下拉列表中选择“lan”接口。

最后，需要将该规则的序号设置为 1，否则客户端的流量将匹配第二条 NAT 规则后进行转换，导致客户端认证失败，如图 2-93 所示。




图 2-93　配置安全规则

配置完成后的规则列表如图 2-94 所示。

安全策略>>安全规则　　跳转到 全部

| 序号 | 规则名 | 源地址 | 目的地址 | 服务 | 类型 | 选项 | 生效 |
|---|---|---|---|---|---|---|---|
| ☐ 1 | allow_auth | 192.168.1.0 | 192.168.1.1 | firewall_auth | ✓ | | ✔ |
| ☐ 2 | nat1 | 192.168.1.200 | any | any | NAT规则 | | ✔ |
| ☐ 3 | nat2 | 192.168.1.0 | any | any | NAT规则 | | ✔ |

图 2-94　配置完成后的规则列表

## 8. 配置客户端认证程序

客户端认证程序在防火墙配套光盘中的 User Auth 文件夹中，双击 auth_client.exe 文件启动该程序，如图 2-95 所示。

在“设置”菜单中选择“服务器”选项，配置认证服务器。服务器地址即为防火墙的地址，端口号使用默认的 9998，如图 2-96 所示。




图 2-95　配置客户端认证程序




图 2-96　配置认证服务器

在“功能”菜单中选择“连接”选项，输入在防火墙中创建的用户名和密码，单击“连接”按钮进行认证，如图 2-97 所示。

软件提示认证成功如图 2-98 所示。




图 2-97　配置认证服务器用户名和密码

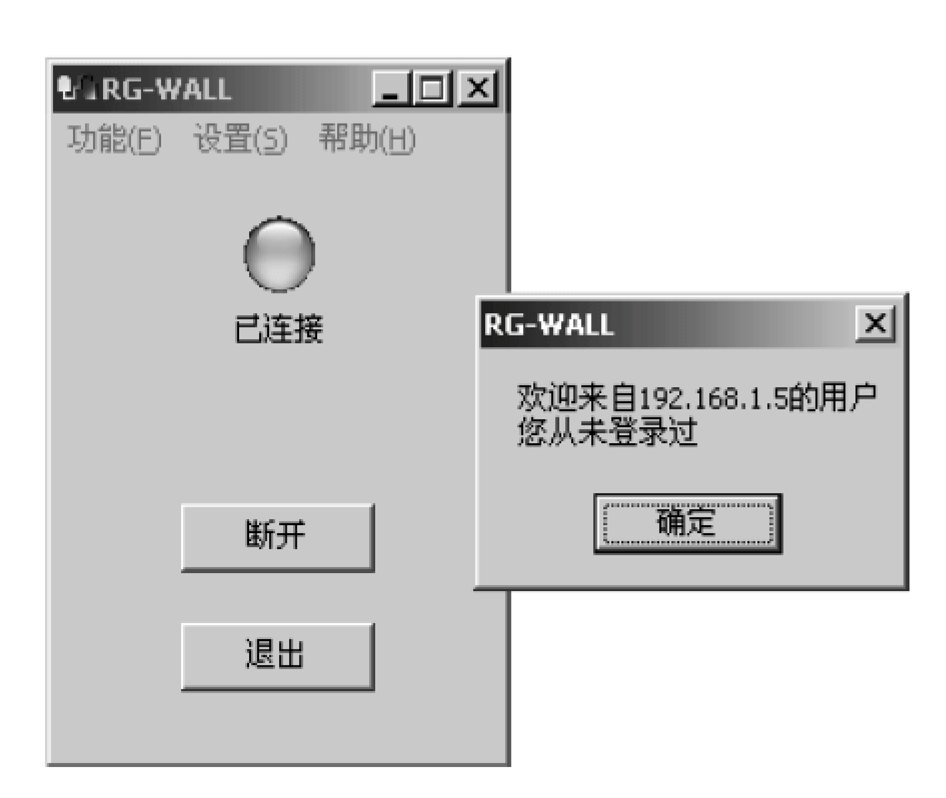



图 2-98　软件提示认证成功

### 9. 验证测试

在内部用户 PC 上访问外部的 FTP 服务器 1.1.1.100，此时可以成功访问，因为已经通过了身份认证，如图 2-99 所示。

```
C:\WINDOWS\system32\cmd.exe - ftp 1.1.1.100
Microsoft Windows XP [版本 5.1.2600]
(C) 版权所有 1985-2001 Microsoft Corp.

C:\Documents and Settings\Administrator>ipconfig

Windows IP Configuration


Ethernet adapter 本地连接:

        Connection-specific DNS Suffix  . :
        IP Address. . . . . . . . . . . . : 192.168.1.5
        Subnet Mask . . . . . . . . . . . : 255.255.255.0
        Default Gateway . . . . . . . . . : 192.168.1.1

C:\Documents and Settings\Administrator>ftp 1.1.1.100
Connected to 1.1.1.100.
220 Serv-U FTP Server v7.2 ready...
User (1.1.1.100:(none)): test
331 User name okay, need password.
Password:
230 User logged in, proceed.
ftp>
```

图 2-99　规则验证测试

## 【注意事项】

防火墙的 NAT 规则是按照顺序进行匹配的，如果数据流匹配到某条规则后，将不再进行后续规则的匹配。所以需要将管理员的 NAT 规则放置在内部用户的 NAT 规则前面，并且将用户认证的包过滤规则放置在内部用户的 NAT 规则前面。

# 2.8　配置防火墙链路负载

## 【实验名称】

配置防火墙链路负载。

## 【实验目的】

利用防火墙来实现双链路负载分担。

## 【背景描述】

某公司原先使用一条广域网链路连接 Internet。随着公司员工的增加，原先的 Internet 链路已经不能满足业务需求，因此公司又向 ISP 申请了一条 Internet 线路。为了合理地利用带宽，避免带宽资源的浪费，公司希望在两个 Internet 链路上进行流量的负载分担。

## 【需求分析】

为了使流量能够在两条链路上进行负载分担,可以使用防火墙提供的策略路由功能。

## 【实验拓扑】

如图 2-100 所示的网络拓扑,企业网络为了合理地利用带宽,避免带宽资源的浪费,在两个 Internet 链路上进行流量的负载分担,使用防火墙提供的策略路由功能,以实现企业网络安全访问需求。

图 2-100　防火墙提供的策略路由来实现流量负载分担的网络拓扑图

## 【实验设备】

两个防火墙连接 Internet 的链路
防火墙　　1 台
PC　　　　1 台
交换机　　1 台

## 【预备知识】

- 网络基础知识。
- 防火墙工作原理。

## 【实验原理】

防火墙的策略路由功能可以实现路由的负载均衡,即到达同一目的地的报文可以指定多个下一跳地址。

## 【实验步骤】

### 1. 配置防火墙接口的 IP 地址

进入防火墙的配置页面,即"网络配置≫接口 IP"页面,单击"添加"按钮,为接口添加 IP 地址。为防火墙的 LAN 接口配置 IP 地址及子网掩码,如图 2-101 所示。

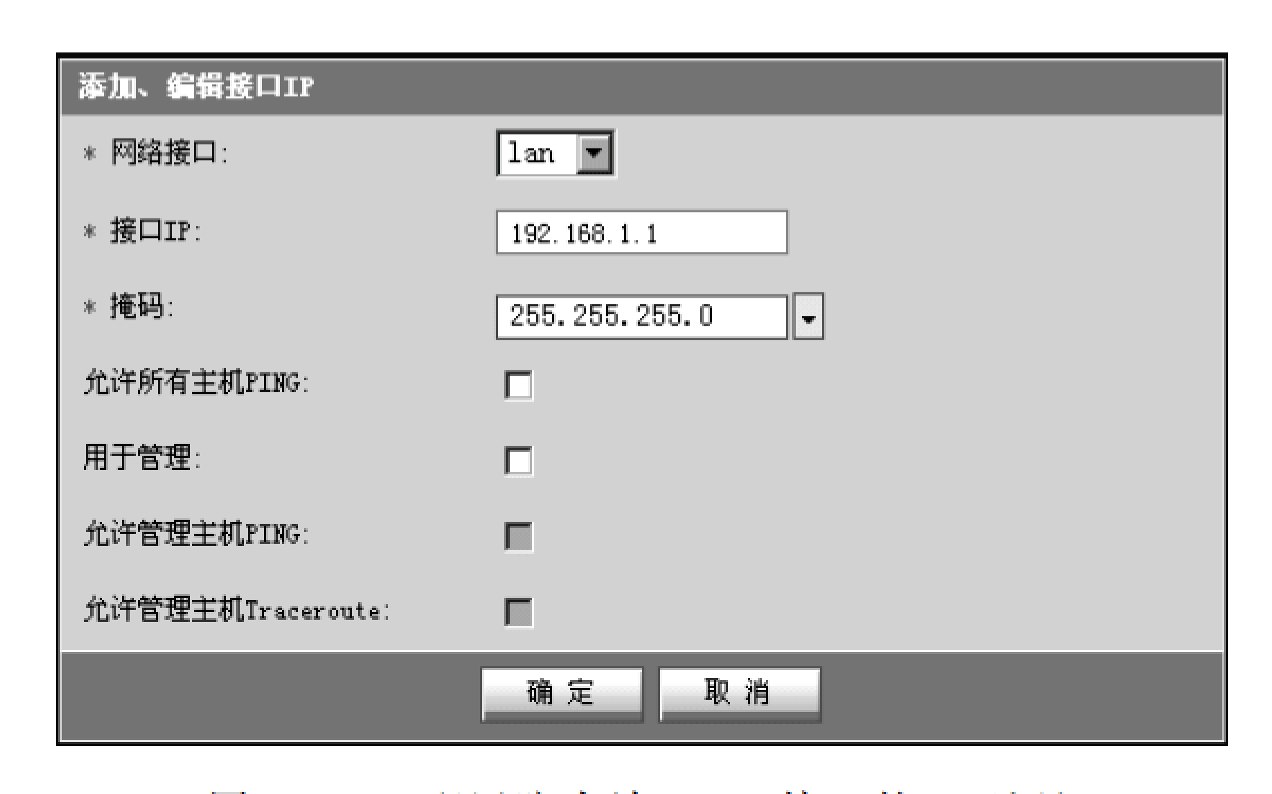



图 2-101　配置防火墙 LAN 接口的 IP 地址

为防火墙的 WAN 接口配置 IP 地址及子网掩码，如图 2-102 所示。

添加、编辑接口IP
* 网络接口：wan
* 接口IP：1.1.1.1
* 掩码：255.255.255.0
允许所有主机PING：
用于管理：
允许管理主机PING：
允许管理主机Traceroute：
确 定　取 消

图 2-102　配置防火墙 WAN 接口的 IP 地址

为防火墙的 WAN1 接口配置 IP 地址及子网掩码，如图 2-103 所示。

添加、编辑接口IP
* 网络接口：wan1
* 接口IP：2.2.2.1
* 掩码：255.255.255.0
允许所有主机PING：
用于管理：
允许管理主机PING：
允许管理主机Traceroute：
确 定　取 消

图 2-103　配置防火墙 WAN1 接口的 IP 地址

### 2. 配置 NAT 规则

进入防火墙配置页面，即“安全策略≫安全规则”页面，单击页面上方的“NAT 规则”按钮，添加 NAT 规则。

在 NAT 规则中，将“源地址转换为”设置为 by_route，表明防火墙将根据路由器来确定转换后的地址，如图 2-104 所示。

### 3. 配置策略路由

进入防火墙配置页面，即“网络配置≫策略路由”页面，单击“添加”按钮配置路由。在策略路由配置框中选择“路由负载均衡”选项，这样我们可以为到达同一个目的地的网络添加多个下一跳地址。

配置到达 Internet 的默认路由 0.0.0.0/0，并将下一跳设置为两个 ISP 的地址，权重都配置为 1，这样流量将在两条链路上进行平分，如图 2-105 所示。




图 2-104　配置防火墙的 NAT 规则




图 2-105　配置防火墙的策略路由

## 【注意事项】

防火墙的负载均衡按照目的地址进行负载，即到达地址 A 的报文走第一条链路，并且后续到达地址 A 的报文也将走第一条链路。到达目的地址 B 的报文走第二条链路，随后到达地址 C 的报文将走第一条链路。

# 2.9　使用防火墙限制连接带宽

## 【实验名称】

使用防火墙限制连接带宽。

## 【实验目的】

利用防火墙对用户连接的带宽进行有效控制。

## 【背景描述】

某企业使用 5M 的广域网链路实现与 Internet 的互联。但是企业的网络管理员发现，最近公司内部一些员工经常下载一些容量很大的文件，导致大量的带宽资源被占用，影响了公司正常业务的开展。公司要求能够尽快解决该问题，限制用户从 Internet 上下载文件所占用的带宽，保证带宽资源被合理地利用。

## 【需求分析】

使用防火墙的带宽限制功能，可以限制每个 IP 地址或者每个子网访问外部服务所占用的带宽。

## 【实验拓扑】

如图 2-106 所示的网络拓扑，企业网络为了限制用户从 Internet 上下载文件所占用的带宽，保证带宽资源被合理地利用，使用防火墙提供的带宽限制功能，限制每个 IP 地址或者每个子网访问外部服务所占用带宽，以实现企业网络安全访问需求规划。

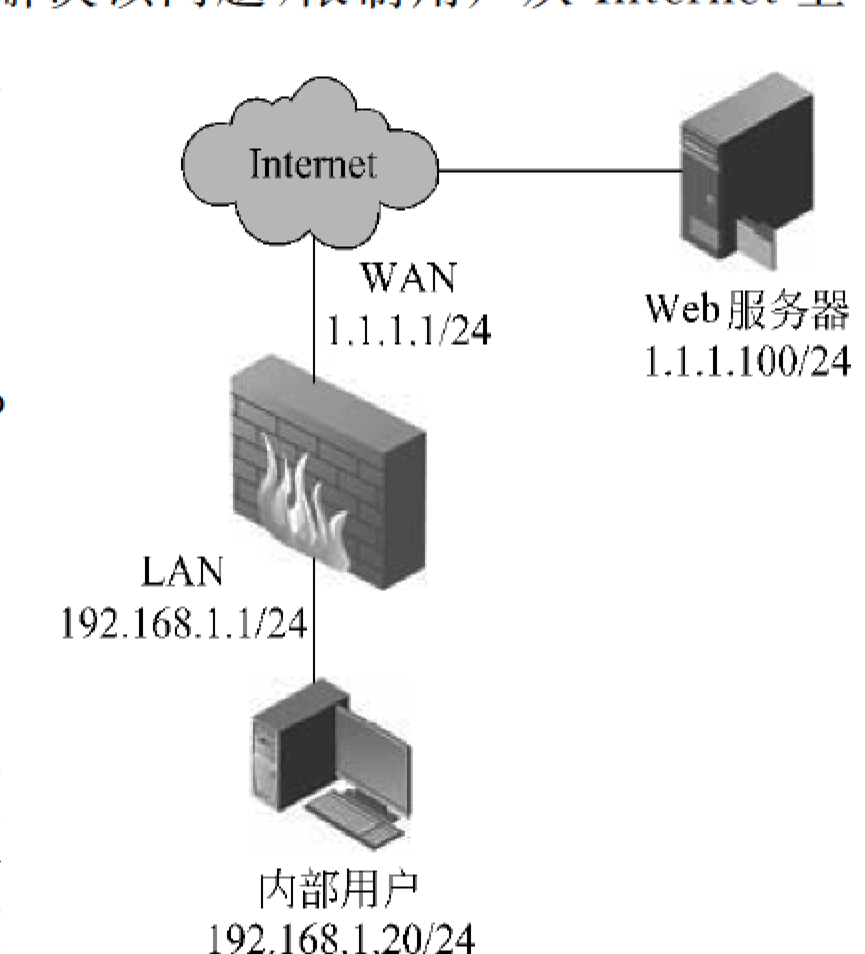



图 2-106　防火墙带宽限制网络访问规划拓扑图

## 【实验设备】

防火墙　　1 台

PC　　　　2 台(其中一台模拟 Internet 中的 Web 服务器)

Web 服务器软件程序

## 【预备知识】

- 网络基础知识。
- 防火墙工作原理。

## 【实验原理】

RG-WALL 防火墙集成了 QoS(服务质量)功能，利用防火墙的带宽控制功能，可以限制每个 IP 地址或者每个子网访问外部网络所占用的带宽。

## 【实验步骤】

### 1. 配置防火墙接口的 IP 地址

进入防火墙的配置页面，即“网络配置≫接口 IP”页面，单击“添加”按钮，为接口添加 IP 地址。为防火墙的 LAN 接口配置 IP 地址及子网掩码，如图 2-107 所示。

为防火墙的 WAN 接口配置 IP 地址及子网掩码，如图 2-108 所示。

添加、编辑接口IP

| | |
|---|---|
| * 网络接口: | lan |
| * 接口IP: | 192.168.1.1 |
| * 掩码: | 255.255.255.0 |
| 允许所有主机PING: | ☐ |
| 用于管理: | ☐ |
| 允许管理主机PING: | ☐ |
| 允许管理主机Traceroute: | ☐ |

确 定　取 消

图 2-107　配置防火墙 LAN 接口的 IP 地址

添加、编辑接口IP

| | |
|---|---|
| * 网络接口: | wan |
| * 接口IP: | 1.1.1.1 |
| * 掩码: | 255.255.255.0 |
| 允许所有主机PING: | ☐ |
| 用于管理: | ☐ |
| 允许管理主机PING: | ☐ |
| 允许管理主机Traceroute: | ☐ |

确 定　取 消

图 2-108　配置防火墙 WAN 接口的 IP 地址

## 2 配置 NAT 规则

进入防火墙配置页面，即“安全策略≫安全规则”页面，单击页面上方的“NAT 规则”按钮，添加 NAT 规则。在 NAT 规则中我们对内部访问外部的 HTTP 流量进行 NAT 转换，如图 2-109 所示。




图 2-109　配置防火墙的 NAT 规则

### 3. 验证测试

在内部用户 PC 上访问外部的 Web 服务器 1.1.1.100,可以成功访问,如图 2-110、图 2-111 所示。

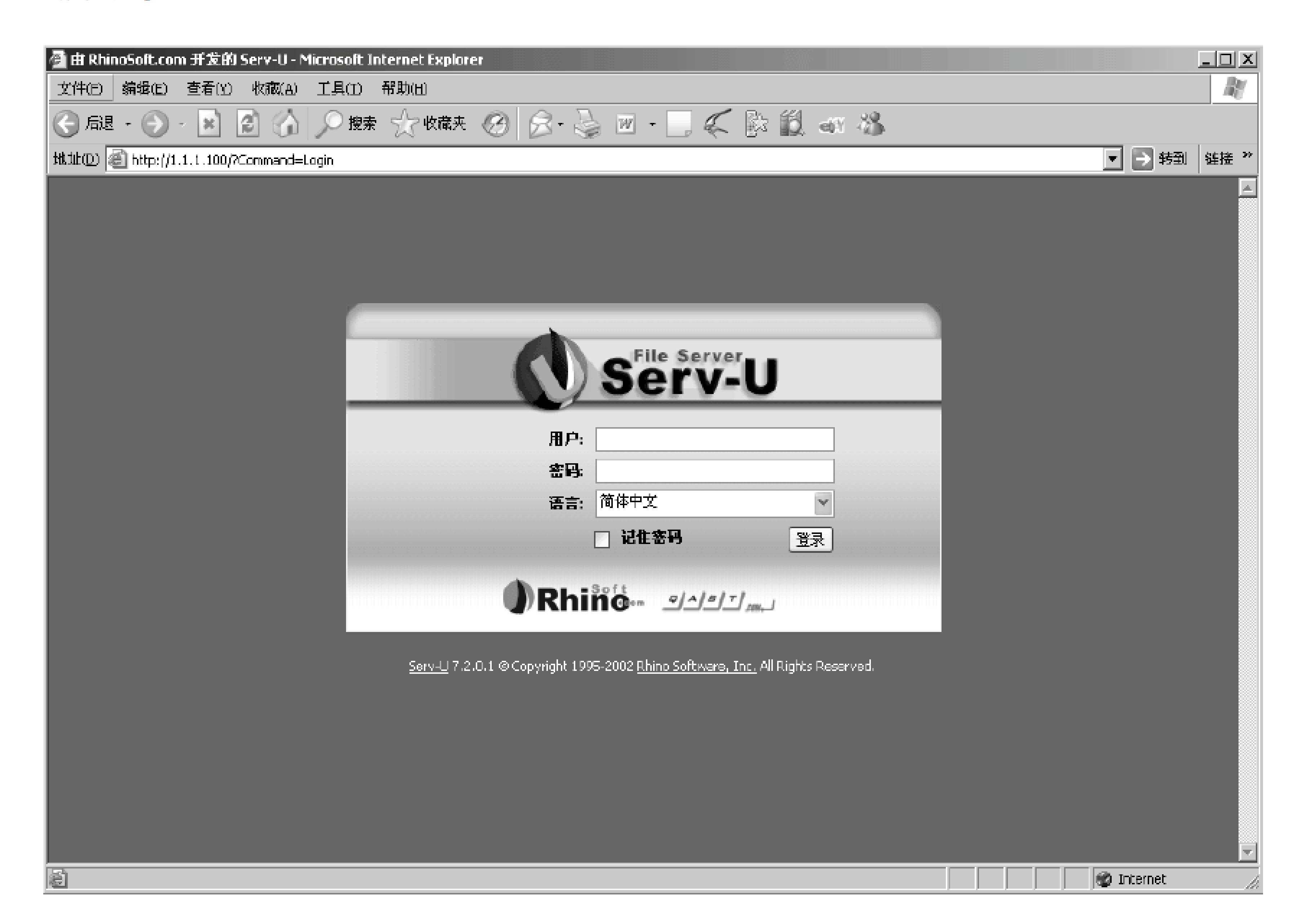



图 2-110　验证测试(1)

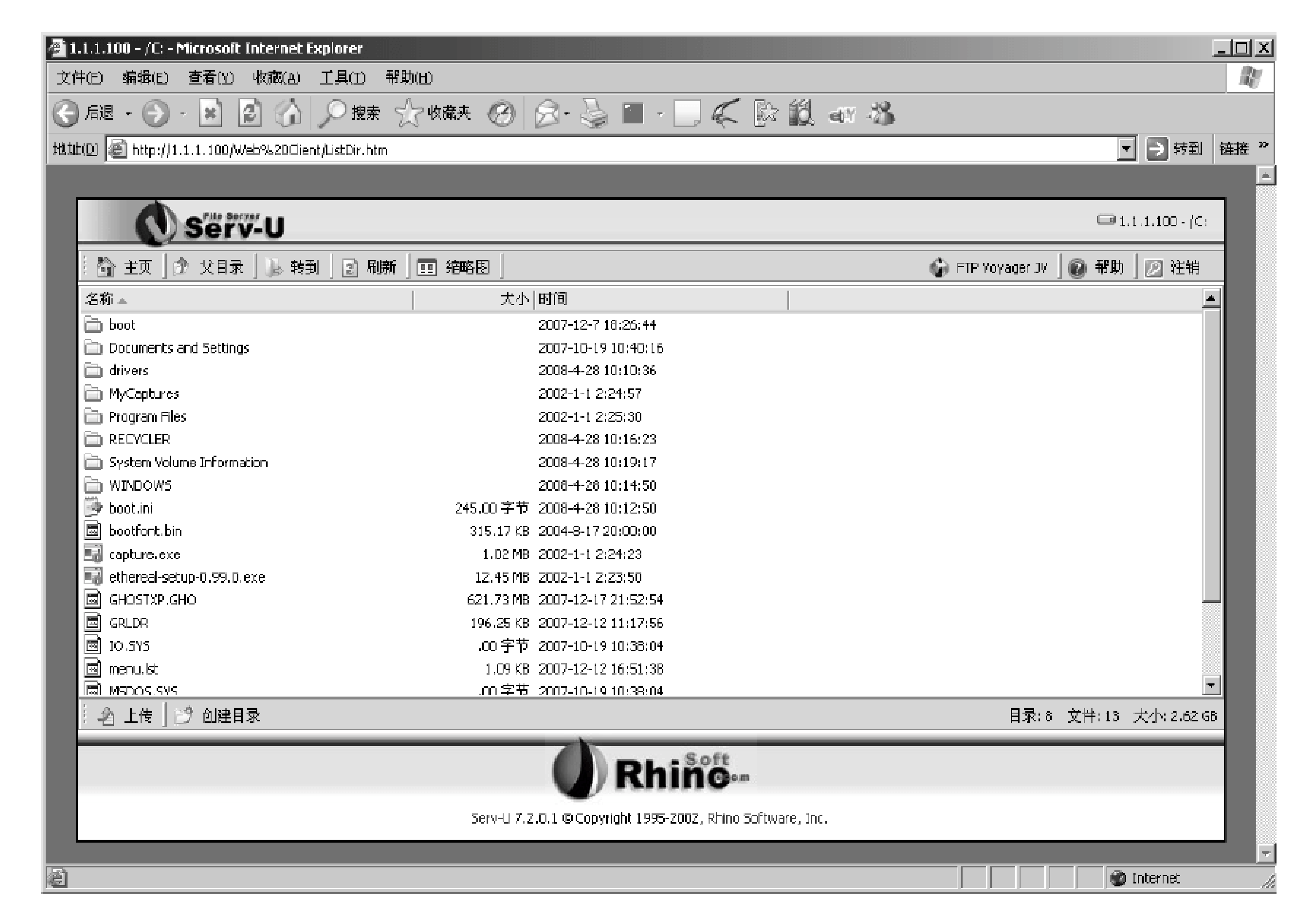



图 2-111　验证测试(2)

使用客户端下载 Web 服务器上的文件,观察下载速率,大约为 2.5MB/s,如图 2-112 所示。

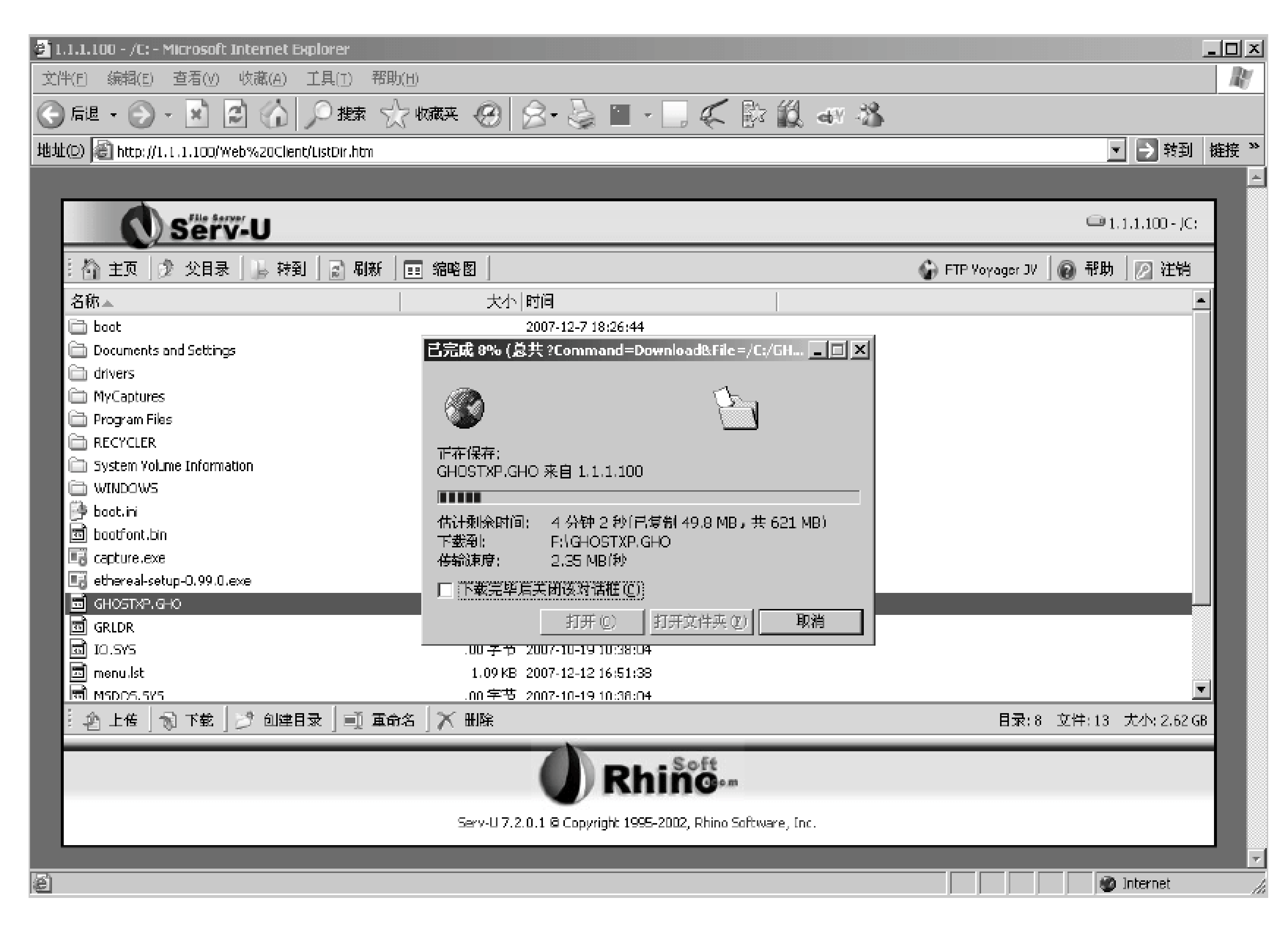



图 2-112 观察下载速率

## 4. 配置带宽列表

进入防火墙配置页面，即“对象定义≫带宽列表”页面，单击页面上的“添加”按钮，创建带宽列表。在带宽列表中配置保证带宽为 256Kbps，最大带宽为 512Kbps，如图 2-113 所示。




图 2-113 配置防火墙的带宽列表

## 5. 应用带宽列表

进入防火墙配置页面，即“安全策略≫安全规则”页面，对之前创建的 NAT 规则进行编辑。在 NAT 规则“流量控制”下拉列表中选择刚才创建的带宽列表 http_limit，如图 2-114 所示。

## 6. 验证测试

在内部用户 PC 上从 Web 服务器下载文件，观察下载速率，最后下载速率稳定在大约 65KB/s，约 520Kbps，与之前设置的最大带宽 512Kbps 相近，如图 2-115 所示。




图 2-114　应用防火墙带宽列表

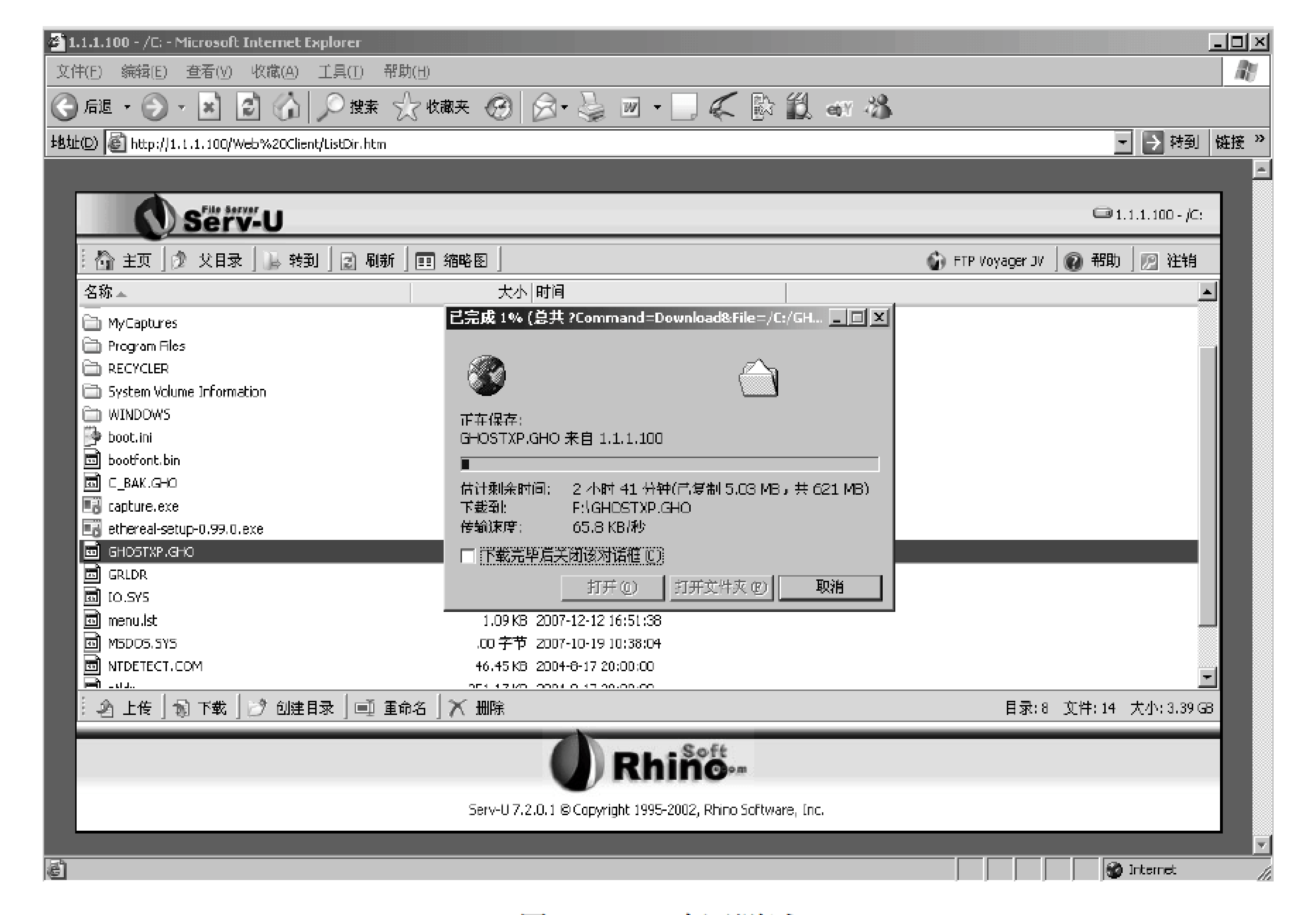



图 2-115　验证测试

## 【注意事项】

- 带宽限制具有一定的偏移量,无法做到完全精确的速率限制。
- 在本实验中由于使用 IP 地址对 Web 服务器进行访问,如果实际中使用域名访问 Web 服务器,还需要对 DNS 解析流量配置 NAT 转换规则。

# 2.10 使用防火墙限制 P2P 流量

## 【实验名称】

使用防火墙限制 P2P 流量。

## 【实验目的】

利用防火墙控制 P2P 流量,保护带宽资源(注:RG-WALL 60 防火墙不支持 P2P 限制)。

## 【背景描述】

某企业使用 1M 的广域网链路实现与 Internet 的互联。但是企业的网络管理员发现,最近公司内部访问 Internet 的速度很慢,有时需要很长时间才能打开一个网页。网络管理员经过对问题的分析和定位,发现此问题是由于一些员工使用 BT 等 P2P 软件进行大量的资源下载而导致的。公司要求能够尽快解决该问题,防止过多的 P2P 流量占用宝贵的带宽资源,影响公司的正常业务。

## 【需求分析】

P2P 软件不仅可以抢占带宽,而且还可以以最大带宽进行数据传输。用防火墙的 P2P 限制功能可以对 P2P 流量进行检测和控制,限制 P2P 流量所占用的带宽。

## 【实验拓扑】

如图 2-116 所示的网络拓扑,是企业网络为了限制用户使用 BT 等 P2P 软件进行大量的资源下载文件所占用的带宽,为保证带宽资源被合理地利用,使用防火墙提供的 P2P 流量限制功能对 P2P 流量进行检测和控制,限制 P2P 流量所占用的带宽,以实现企业网络安全访问需求规划。

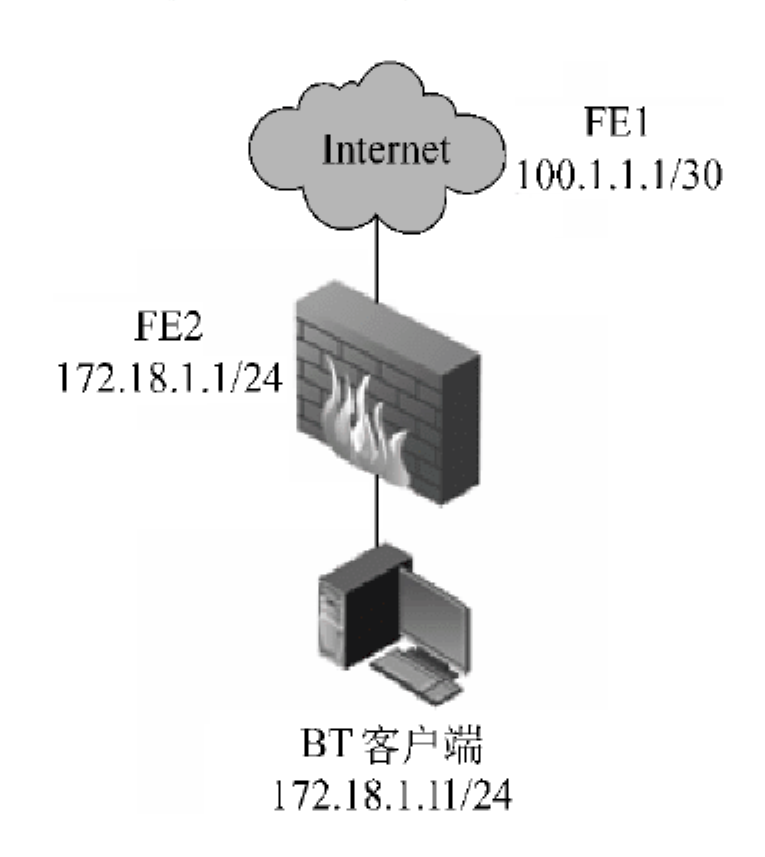



图 2-116 防火墙的 P2P 流量限制网络规划拓扑图

## 【实验设备】

防火墙连接到 Internet 的链路
防火墙 1 台
PC(安装 BT 客户端软件) 1 台

## 【预备知识】

- 网络基础知识。
- 防火墙工作原理。

## 【实验原理】

P2P 技术具备客户端和服务器双重特性，可以同时作为服务使用者和服务提供者。由于 P2P 技术的飞速发展，现在 Internet 上 70%的流量都是 P2P 的流量。由于 P2P 技术在下载的同时，也需要上传流量，导致用户的下行流量和上行流量都很大，从而 P2P 流量造成了网络的极度拥塞。

RG-WALL 防火墙对 P2P 软件采用深度检测的方法，可以精确地识别 P2P 流量，以达到对 P2P 流量进行控制的目的。

## 【实验步骤】

### 1. 配置防火墙接口的地址

如图 2-117 所示，配置 FE1 接口的地址。

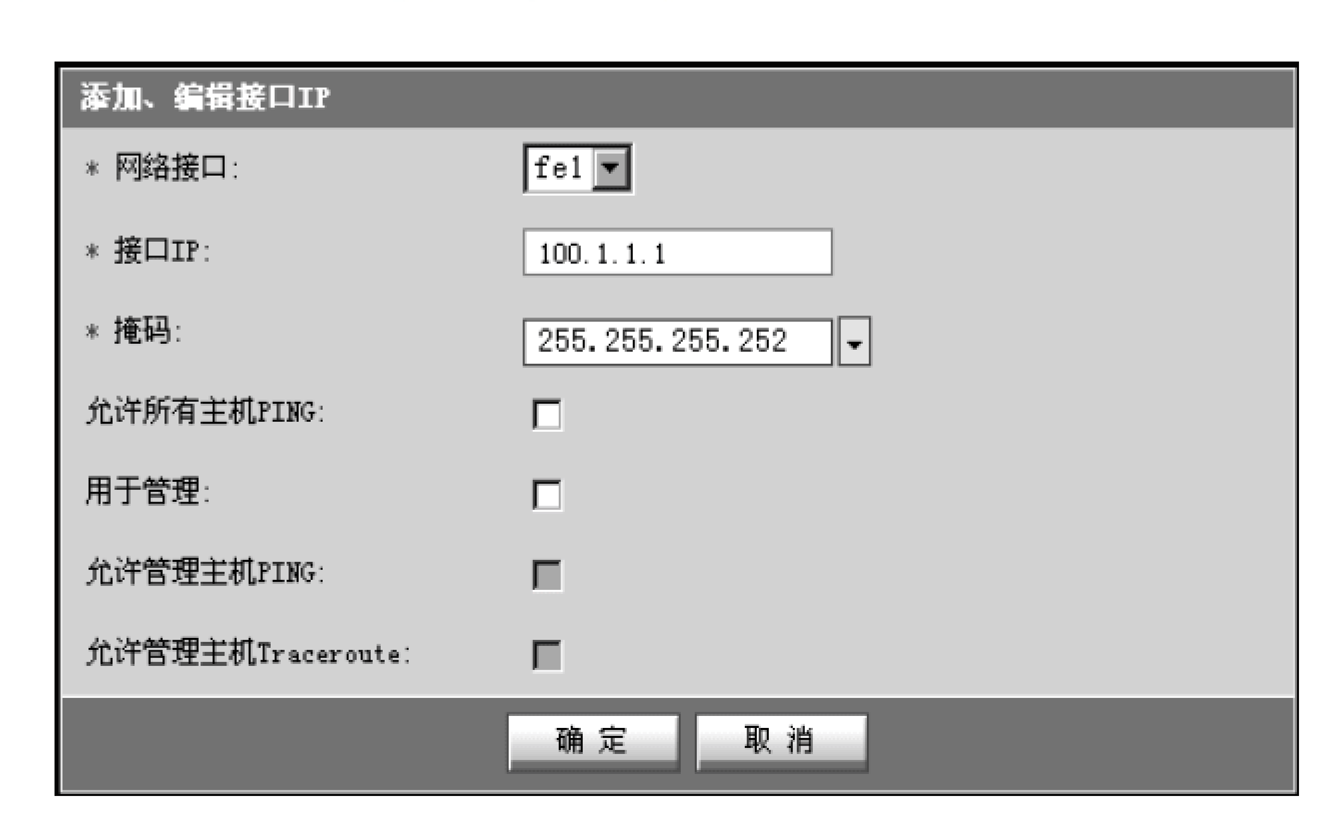



图 2-117　配置防火墙 FE1 接口的地址

配置 FE2 接口的地址，如图 2-118 所示。

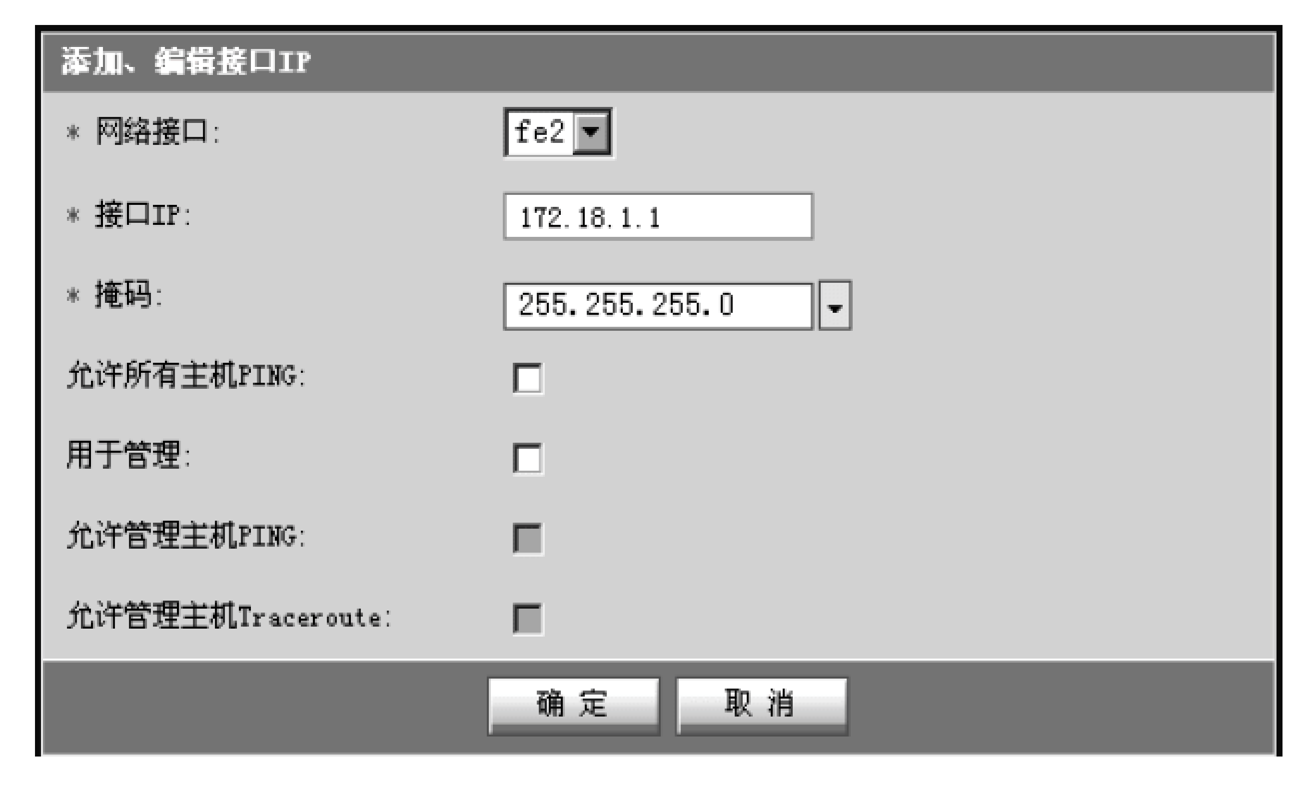



图 2-118　配置防火墙 FE2 接口的地址

### 2 配置 NAT 转换规则

配置 NAT 规则，使内部用户可以访问 Internet，如图 2-119 所示。




图 2-119　配置防火墙的 NAT 转换规则

## 3. 验证测试

验证客户端可以访问 Internet，并且可以用 BT 下载 Internet 上的资源，记录下载带宽，例如，400Kb/s。

## 4. 配置带宽列表

进入防火墙配置页面，即“对象定义≫带宽列表”页面，可以看到系统已经预定义了一个名为 p2p_band 的带宽列表，如图 2-120 所示。




图 2-120　配置防火墙带宽列表(1)

单击后面的编辑图标，可以看到预先定义的保证带宽为 60Kb/s，最大带宽为 160Kb/s。在本实验中我们设置保证带宽为 60Kb/s，最大带宽为 80Kb/s，如图 2-121 所示。




图 2-121　配置防火墙带宽列表(2)

### 5. 配置 P2P 限制

进入防火墙配置页面，即“安全策略≫P2P 限制”页面，在 bt 协议的下拉列表中选择“允许使用且进行流量控制”选项，并在“流量控制”下拉列表中选择之前定义的带宽列表 p2p_band，如图 2-122 所示。




图 2-122　配置防火墙的 P2P 带宽限制

### 6. 配置规则应用 P2P 限制

在之前配置的 NAT 规则中，在高级选项的“深度行为检测”区域中勾选“P2P 限制”复选框，以启用该规则的 P2P 检测和控制，如图 2-123 所示。

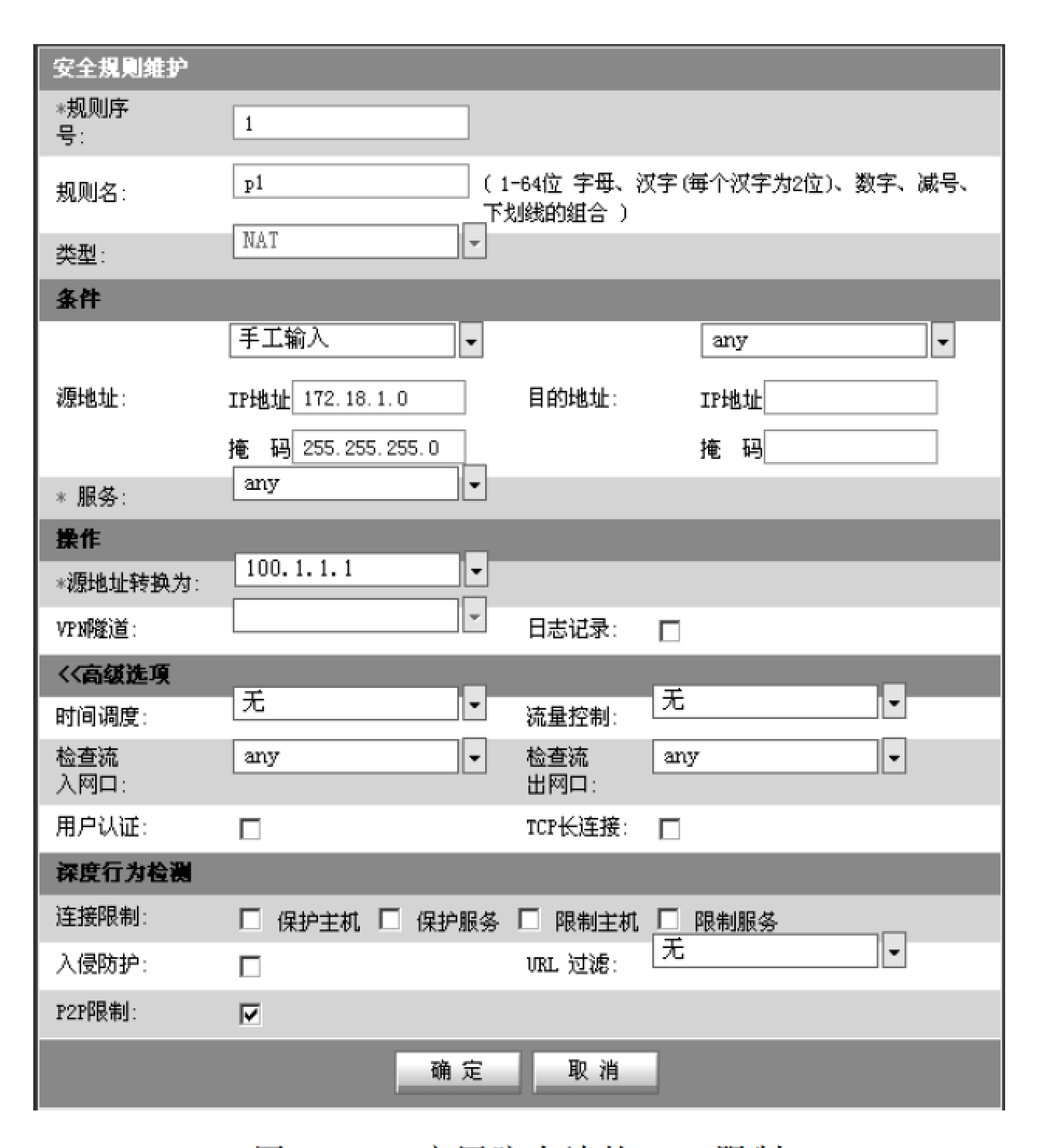



图 2-123　应用防火墙的 P2P 限制

### 7. 验证测试

在客户端上使用 BT 进行文件下载，可以看到下载速率在 60Kb/s～80Kb/s 之间。

## 【注意事项】

- P2P 和带宽限制具有一定的偏移量，无法做到完全精确的速率限制。
- 在本实验中没有给出防火墙路由的配置，需要根据实际网络情况在防火墙上配置浏览 Internet 的路由(通常是默认路由)。

# 2.11 使用防火墙防止 DoS 攻击

## 【实验名称】

使用防火墙防止 DoS 攻击。

## 【实验目的】

利用防火墙的抗攻击功能防止 SYN Flood 攻击。

## 【背景描述】

某公司使用防火墙作为网络出口设备连接到 Internet，并且公司内部有一台对外提供服务的 FTP 服务器。最近网络管理员发现在 Internet 中有人向 FTP 服务器发起 SYN Flood 攻击，造成 FTP 上存在大量的半开放连接，消耗了服务器的系统资源。

## 【需求分析】

要防止来自外部网络的 DoS 攻击，可以使用防火墙的抗攻击功能。

## 【实验拓扑】

如图 2-124 所示的网络拓扑，企业网络为了限制有人向 FTP 服务器发起 SYN Flood 攻击，造成 FTP 上存在大量的半开放连接，消耗了服务器的系统资源，希望利用防火墙的抗攻击功能防止 SYN Flood 攻击，从而防止来自外部网络的 DoS 攻击，以实现企业网络安全访问需求规划。

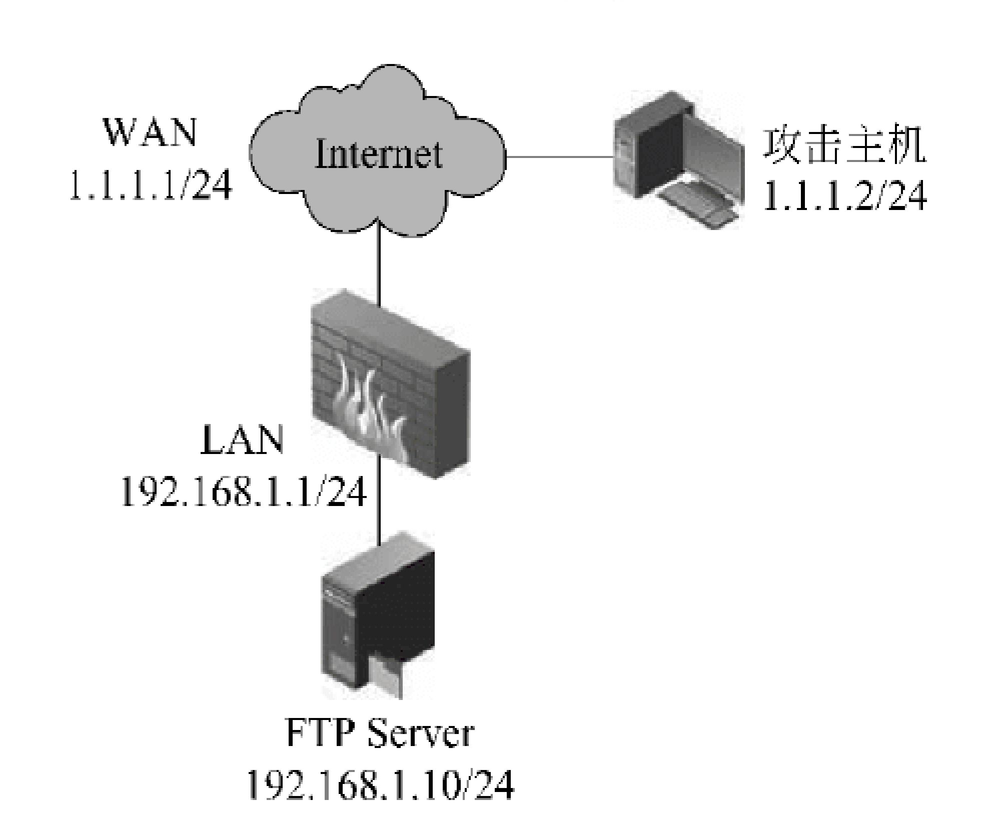



图 2-124　防火墙的抗攻击功能网络规划拓扑图

## 【实验设备】

| | |
|---|---|
| 防火墙 | 1 台 |
| PC | 2 台(一台作为 FTP 服务器；另一台模拟外部网络的攻击主机) |

FTP 服务器软件程序　SYN Flood 攻击软件程序

## 【预备知识】

- 网络基础知识。
- 防火墙工作原理。
- DoS 攻击原理。

## 【实验原理】

SYN Flood 是一种常见的 DoS 攻击,这种攻击通过使用伪造的源 IP 地址,向目标主机(被攻击端)发送大量的 TCP SYN 报文。目标主机接收到 SYN 报文后,会向伪造的源地址回应 TCP SYN_ACK 报文以等待发送端的 ACK 报文来建立连接。但是由于发送端的地址是伪造的,所以被攻击端永远不会收到合法的 ACK 报文,这将造成被攻击端建立大量的半开放连接,消耗大量的系统资源,导致不能提供正常的服务。

防火墙的抗攻击功能可以对 SYN Flood 攻击进行检测,阻止大量的 TCP SYN 报文到达被攻击端,保护内部主机的资源。

## 【实验步骤】

### 1. 配置防火墙接口的 IP 地址

进入防火墙的配置页面,即"网络配置≫接口 IP"页面,单击"添加"按钮,为接口添加 IP 地址。

为防火墙的 LAN 接口配置 IP 地址及子网掩码,如图 2-125 所示。

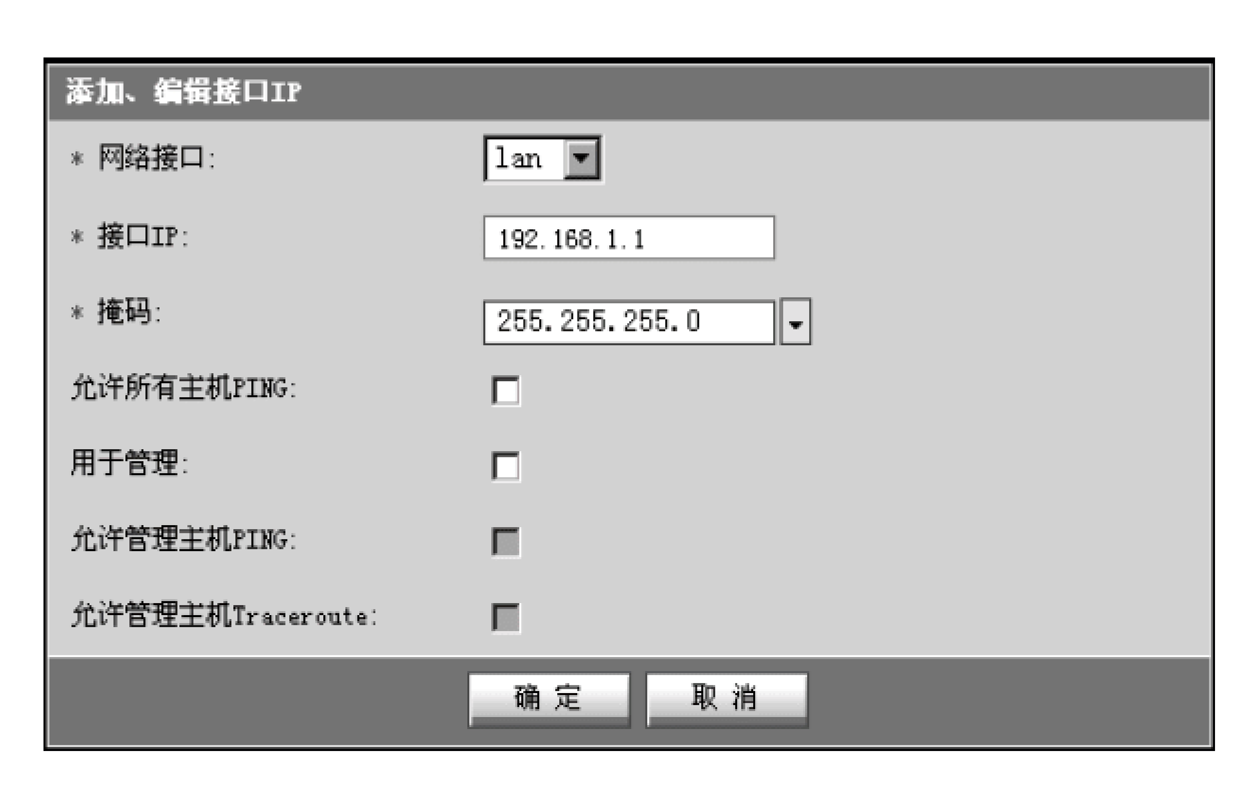



图 2-125　配置防火墙 LAN 接口的 IP 地址

为防火墙的 WAN 接口配置 IP 地址及子网掩码,如图 2-126 所示。

### 2 配置端口映射规则

为了使 Internet 中的用户可以访问到内部的 FTP 服务器,需要在防火墙上使用端口映射规则,将 FTP 服务器发布到 Internet 中。

进入防火墙配置页面,即"安全策略≫安全规则"页面,单击页面上方的"端口映射规则"按钮,添加端口映射规则。规则中的"公开地址"为防火墙外部接口(WAN)的地址;

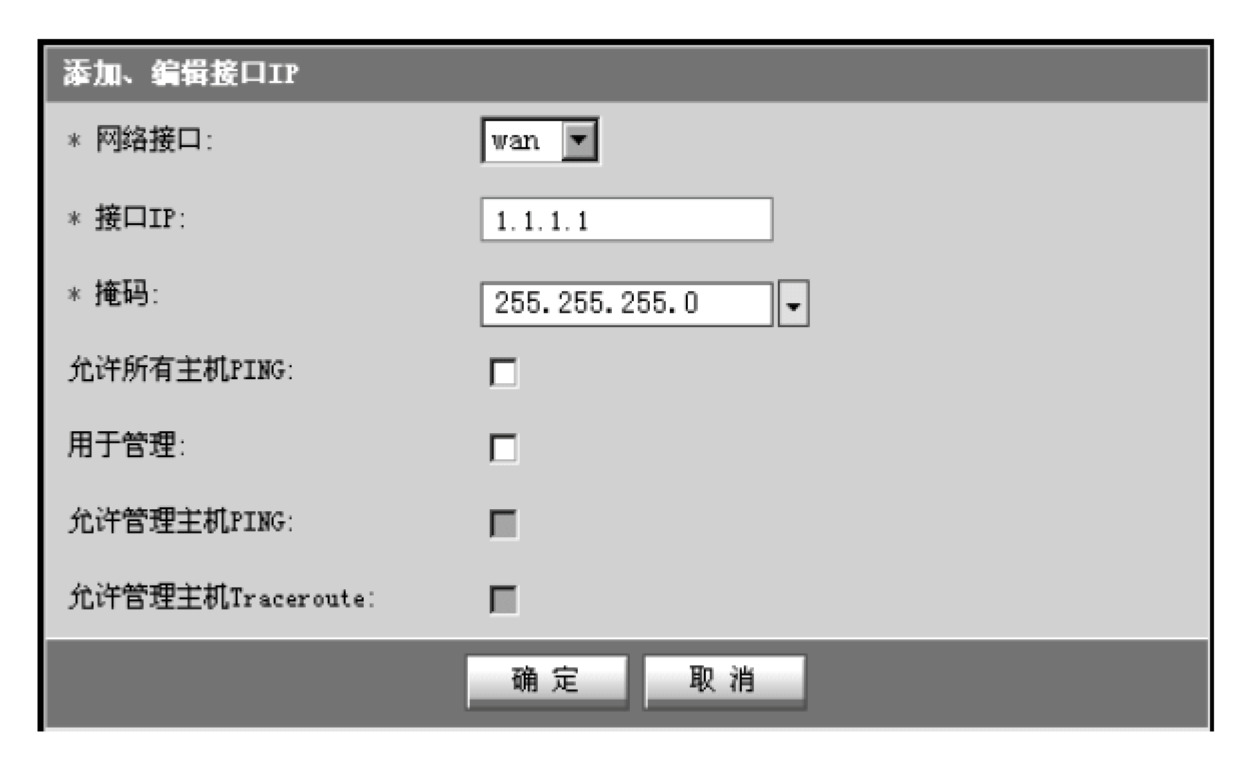



图 2-126　配置防火墙 WAN 接口的 IP 地址

“内部地址”为内部 FTP 服务器的地址;“内部服务”为 FTP 服务器提供 FTP 服务使用的端口号,这里使用默认的 21 端口(FTP);“对外服务”为 Internet 用户访问 FTP 服务器时使用的在外部看到的端口号,这里也使用默认的 21 端口(FTP),如图 2-127 所示。

端口映射规则维护
满足条件
规则名: pnat1 ( 1-15位 字母、数字、减号、下划线的组合 )
源地址: IP地址 掩 码　　* 公开地址: 1.1.1.1
源地址转换为:　　* 内部地址: 手工输入 IP地址 192.168.1.10
* 对外服务: ftp　　* 内部服务: ftp
执行动作
检查流入网口: wan　　检查流出网口: lan
时间调度:　　流量控制:
用户认证:　　日志记录:
隧道名:　　序号: 1
连接限制: 保护主机 保护服务 限制主机 限制服务
添加下一条　确 定　取 消

图 2-127　配置防火墙的端口映射规则

### 3. 验证测试

在内部 PC 上安装好 FTP Server 程序,并进行相应的配置。在外部 PC 上测试访问 FTP 服务器的连通性,注意这里使用的 FTP 目标地址为 1.1.1.1。防火墙将其发送到 1.1.1.1,端口为 21 的请求重定向到内部的 FTP 服务器。

外部 PC 可以通过预先设置的用户名和密码登录 FTP 服务器,如图 2-128 所示。

### 4. 实施 SYN Flood 攻击

在外部 PC 上使用 SYN Flood 连接工具向 FTP 服务器发起攻击。此时在 FTP 服务器上通过 Windows 命令 netstat -an 可以看到外部主机与 FTP 服务器的 21 端口建立了大量的半开放连接,状态为 SYN_RECEIVED,如图 2-129 所示。

```
C:\WINDOWS\system32\cmd.exe - ftp 1.1.1.1
Microsoft Windows XP [版本 5.1.2600]
(C) 版权所有 1985-2001 Microsoft Corp.

C:\Documents and Settings\Administrator>ftp 1.1.1.1
Connected to 1.1.1.1.
220 Serv-U FTP Server v7.2 ready...
User (1.1.1.1:(none)): test
331 User name okay, need password.
Password:
230 User logged in, proceed.
ftp>
```

图 2-128　验证测试

```
C:\WINDOWS\system32\cmd.exe
  TCP    192.168.1.10:21        1.1.1.3:1024           SYN_RECEIVED
  TCP    192.168.1.10:21        1.1.1.4:1025           SYN_RECEIVED
  TCP    192.168.1.10:21        1.1.1.5:1026           SYN_RECEIVED
  TCP    192.168.1.10:21        1.1.1.6:1027           SYN_RECEIVED
  TCP    192.168.1.10:21        1.1.1.7:1028           SYN_RECEIVED
  TCP    192.168.1.10:21        1.1.1.8:1029           SYN_RECEIVED
  TCP    192.168.1.10:21        1.1.1.9:1030           SYN_RECEIVED
  TCP    192.168.1.10:21        1.1.1.10:1031          SYN_RECEIVED
  TCP    192.168.1.10:21        1.1.1.11:1032          SYN_RECEIVED
  TCP    192.168.1.10:21        1.1.1.12:1033          SYN_RECEIVED
  TCP    192.168.1.10:21        1.1.1.13:1034          SYN_RECEIVED
  TCP    192.168.1.10:21        1.1.1.14:1035          SYN_RECEIVED
  TCP    192.168.1.10:21        1.1.1.15:1036          SYN_RECEIVED
  TCP    192.168.1.10:21        1.1.1.16:1037          SYN_RECEIVED
  TCP    192.168.1.10:21        1.1.1.17:1038          SYN_RECEIVED
  TCP    192.168.1.10:21        1.1.1.18:1039          SYN_RECEIVED
  TCP    192.168.1.10:21        1.1.1.19:1040          SYN_RECEIVED
  TCP    192.168.1.10:21        1.1.1.20:1041          SYN_RECEIVED
  TCP    192.168.1.10:21        1.1.1.21:1042          SYN_RECEIVED
  TCP    192.168.1.10:21        1.1.1.22:1043          SYN_RECEIVED
  TCP    192.168.1.10:21        1.1.1.23:1044          SYN_RECEIVED
  TCP    192.168.1.10:21        1.1.1.24:1045          SYN_RECEIVED
  TCP    192.168.1.10:21        1.1.1.25:1046          SYN_RECEIVED
  TCP    192.168.1.10:21        1.1.1.26:1047          SYN_RECEIVED
  TCP    192.168.1.10:21        1.1.1.27:1048          SYN_RECEIVED
```

图 2-129　外部 PC 实施 SYN Flood 攻击

### 5. 配置抗攻击

进入防火墙配置页面，即“安全策略≫抗攻击”页面，单击 WAN 接口后面的操作图标，如图 2-130 所示。

安全策略>>抗攻击

| 接口名称 | 启用 | SYN Flood | ICMP Flood | Ping of Death | UDP Flood | PING SWEEP | TCP端口扫描 | UDP端口扫描 | WinNuke | 操作 |
|---|---|---|---|---|---|---|---|---|---|---|
| dmz | × | × | × | × | × | × | × | × | × | |
| lan | × | × | × | × | × | × | × | × | × | |
| wan | × | × | × | × | × | × | × | × | × | |
| wan1 | × | × | × | × | × | × | × | × | × | |

图 2-130　配置防火墙的抗攻击功能

启用抗攻击功能，并开启抗 SYN Flood 攻击选项，设置 SYN 包速率阈值为 10pps（小于实际攻击端的发包速率），如图 2-131 所示。

### 6. 验证测试

在外部 PC 上使用 SYN Flood 连接工具再次向 FTP 服务器发起攻击。此时在 FTP 服务器上通过 Windows 命令 netstat -an 可以看到外部主机与 FTP 服务器的 21 端口只建立了少量的半开放连接（大约 10 个），其他所有的 SYN Flood 攻击报文已经被防火墙阻断，如图 2-132 所示。




图 2-131　启用防火墙的抗攻击功能

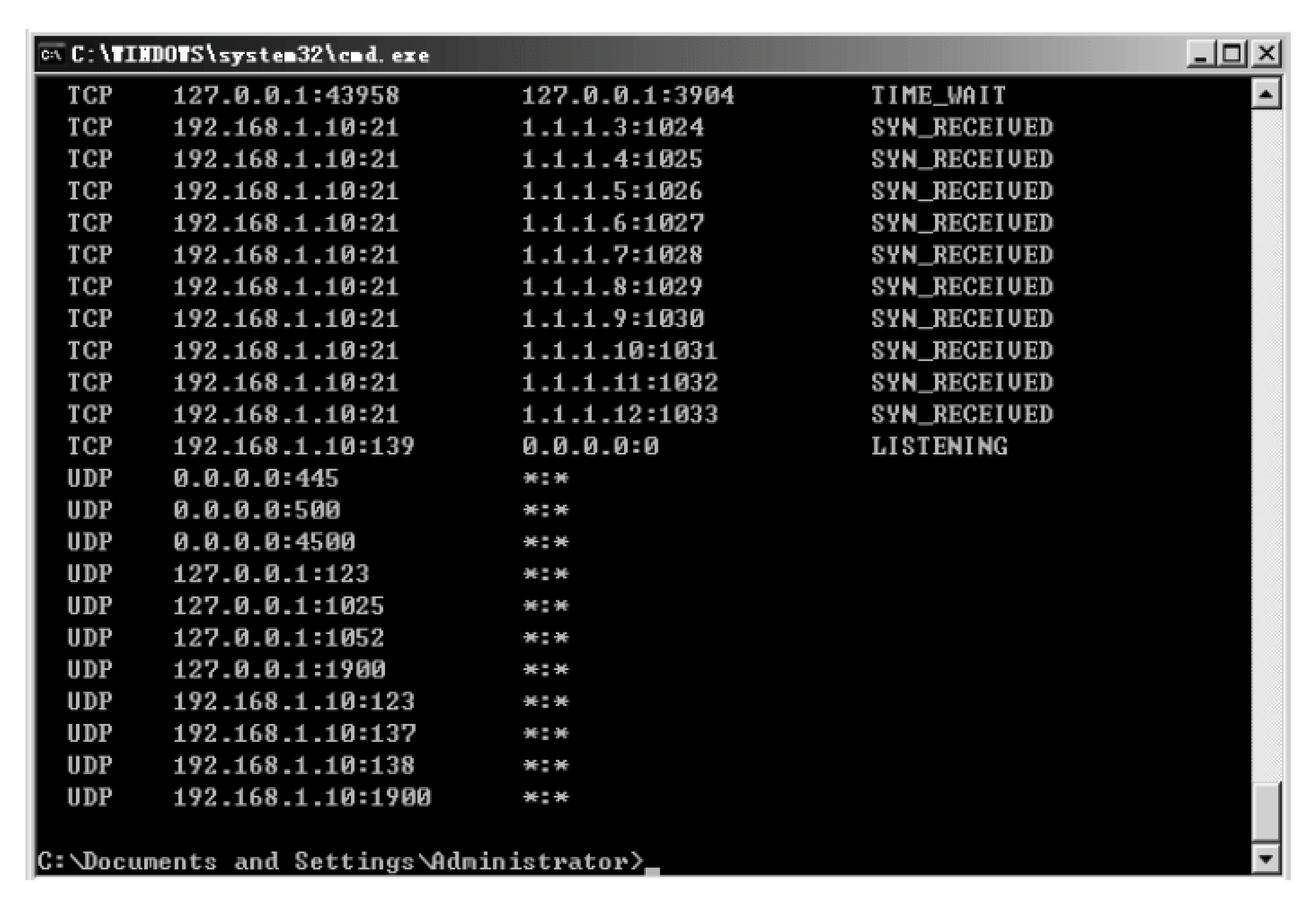



图 2-132　验证防火墙抗攻击测试

## 【注意事项】

- 设置的防火墙 SYN Flood 检测阈值(SYN 包速率)要小于实际攻击端的发包速率。
- 防火墙是根据 SYN 报文速率对 SYN Flood 攻击进行检测的,所以防火墙在接收报文时会有采样的时间,这段时间内部分攻击报文可能会通过防火墙,在目的端造成少量的半连接。
- 检测阈值不要设置得过小,否则可能导致正常的连接请求无法建立。







# 入侵检测技术安全

# 第3章 入侵检测设备基础知识

随着网络安全风险系数不断提高,曾经作为最主要的安全防范手段的防火墙,已经不能满足人们对网络安全的需求。仅仅使用防火墙来保护网络的安全还远远不够,原因在于:

- 网络的入侵者可寻找防火墙的漏洞;
- 网络的入侵者可能就在防火墙内;
- 由于性能的限制,防火墙通常不能提供实时的入侵检测能力。

作为对防火墙的有益补充,入侵检测系统 IDS 能够帮助网络系统快速发现网络攻击的发生,从而扩展系统管理员的安全管理能力(包括安全审计、监视、进攻识别和响应),提高了信息安全基础结构的完整性。IDS 被认为是防火墙之后的第二道安全闸门,它能在不影响网络性能的情况下,对网络进行监听,从而提供对来自内部攻击、外部攻击和误操作的实时保护。

IDS 这一概念最先由 James P. Anderson 在 1980 年 4 月为美国空军做的一份题为《计算机安全威胁监控与监视》的技术报告中提出。此后,经历 20 余年的发展,IDS 终于发展成熟,发展成为基于网络的 IDS 和基于主机的 IDS 两大阵营,并且随着入侵事件的愈演愈烈而逐渐成为安全市场主角。有人将 IDS 产品比作为继杀毒和防火墙产品之后安全领域的第三战场。前两个战场已处于酣战之中,IDS 领域将成为今后一段时期安全厂商角力的主战场。

## 3.1 什么是入侵检测系统

IDS 是英文“Intrusion Detection Systems”的缩写,中文意思是“入侵检测系统”。专业上讲就是依照一定的安全策略,对网络、系统的运行状况进行监视,尽可能发现各种攻击企图、攻击行为或者攻击结果,以保证网络系统资源的机密性、完整性和可用性。做一个形象的比喻:假如防火墙是一幢大楼的门锁,那么 IDS 就是这幢大楼里的监视系统。一旦小偷爬窗进入大楼或内部人员有越界行为,只有实时监视系统才能发现情况并发出警告,IDS 设备如图 3-1 所示。

通过在网络中安装防火墙,可以阻挡一般性的网络攻击行为,采用 IDS 入侵防护系统,则可以对越过防火墙的攻击行为,以及来自网络内部的违规操作进行监测和响应,相当于为网络提供第二套保护机制。入侵检测系统多安置在防火墙之后,对网络活动进行实时检测。在很多情况下,由于可以记录和禁止网络活动,所以入侵检测系统是防火墙



图 3-1 入侵检测系统硬件设备

的延续。它们可以和防火墙以及路由器配合工作。如 IDS 可以通过配置来禁止从防火墙外部进入的恶意流量,独立于防火墙而开展工作的。

入侵检测系统 IDS 与系统扫描器 system scanner 不同。系统扫描器是根据攻击特征数据库来扫描系统漏洞的,它更关注配置上的漏洞而不是当前进出主机的流量。在遭受攻击的主机上,即使正在运行扫描程序,也无法识别这种攻击。IDS 扫描当前网络的活动、监视和记录网络的流量,根据定义好的规则来过滤从主机网卡到网线上的流量,提供实时报警。网络扫描器只检测主机上先前设置的漏洞,而 IDS 监视和记录网络流量。如果在同一台主机上运行 IDS 和扫描器,配置合理的 IDS 会发出许多报警。

不同于防火墙,IDS 入侵检测系统是一个监听设备,没有跨接在任何链路上,无须网络流量流经它便可以工作。因此,对 IDS 的部署,唯一的要求是:IDS 应当挂接在所有所关注流量都必须流经的链路上。在这里,"所关注流量"指的是来自高危网络区域的访问流量和需要进行统计、监视的网络报文。在如今的网络拓扑中,已经很难找到以前的 Hub 式的共享介质冲突域的网络,绝大部分的网络区域都已经全面升级到交换式的网络结构。因此,IDS 在交换式网络中的位置一般选择为:(1)尽可能靠近攻击源;(2)尽可能靠近受保护资源。

这些位置通常是:在服务器区域交换机上,或者在 Internet 接入路由器之后第一台交换机上,或者在重点保护网段局域网交换机上,经典的入侵检测系统部署方式如图 3-2 所示。

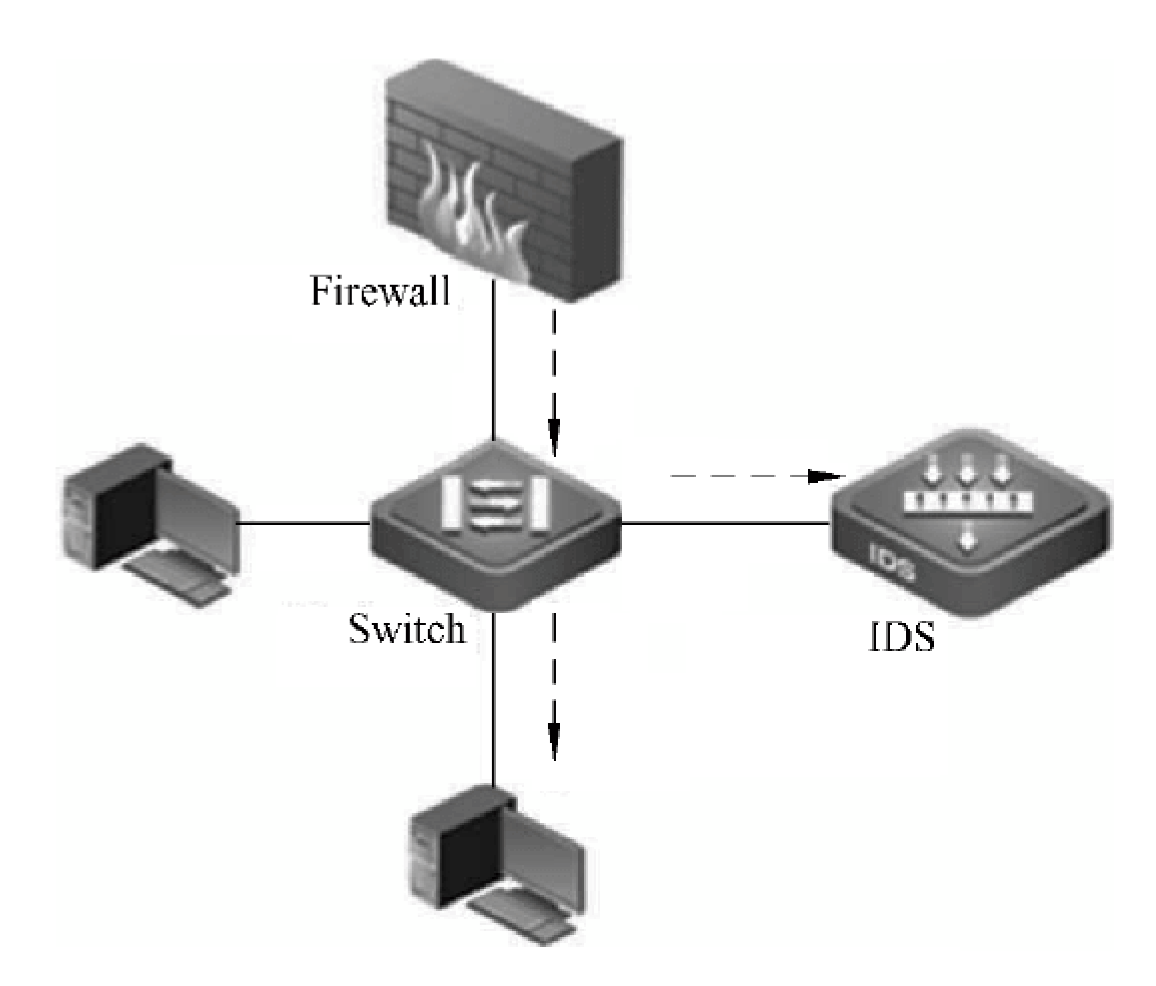



图 3-2 IDS 的部署网络拓扑图

## 3.2　入侵检测系统功能

大多数的入侵检测系统 IDS 可以提供关于网络流量非常详尽的分析，它们可以监视任何定义好的流量，如对 FTP、HTTP 和 Telnet 流量都有默认的设置，对其他的流量如 NetBus、本地和远程登录等，可以自己定制策略。

常见的入侵检测系统检测功能如下：

### 1. 网络流量管理

大多数的入侵检测系统 IDS 允许记录、报告和禁止几乎所有形式的网络访问。还可以用它监视某一台主机上通过的所有网络流量。如定义了策略和规则，在设备上获得 FTP、SMTP、Telnet 和任何其他的流量，这种策略和规则有助于追查该连接和确定网络上发生过什么，或现在正在发生什么。这在需要确定网络中策略实施的一致性时是非常有效的工具。

虽然入侵检测系统 IDS 是网络中安全管理人员或审计人员非常有价值的工具，但公司内网中的用户同样可以安装像 eTrust Intrusion Detection 或 Intrude Alert 这样的程序来访问重要的信息。攻击者不仅可以读取未加密的邮件，还可以嗅探密码和收集重要的协议方面的信息。所以实施整网安全工作还要检查在网络中是否有类似的程序在运行。

### 2. 系统扫描

入侵检测系统 IDS 设备可以在网络中对不同的应用实施控制，从操作系统到扫描器、IDS 程序和防火墙。许多安全专家将这些应用和 IDS 结合起来。

### 3. 追踪

入侵检测系统 IDS 设备所能做的不仅仅是记录安全事件，它还可以确定安全事件发生的位置。通过追踪来源，可以更多地了解攻击者。IDS 检测设备记录下的日志不仅可以记录攻击过程，同时也有助于确定解决方案。

## 3.3　入侵检测系统工作原理

早期的 IDS 设备仅仅是一个监听系统，IDS 可以将位于与 IDS 连接在同一网络中的交换机/Hub 和服务器的访问、操作全部记录下来以供分析使用。跟常用的 Windows 操作系统的事件查看器类似，本质上入侵检测系统 IDS 是一个典型的“窥探设备”，它不跨接多个物理网段(通常只有一个监听端口)，无须转发任何流量，只在网络上被动地、无声息地收集它所关心的报文，如图 3-3 所示。

IDS 就像交通灯、摄像头一样，对攻击者常规的入侵行为做很好的监测，对网络安全有一定的保护作用。入侵检测系统具有的作用主要表现在以下几方面：

- 通过检测和记录网络中的安全违规行为，防止网络入侵事件的发生；
- 检测其他安全措施未能阻止的攻击或安全违规行为；

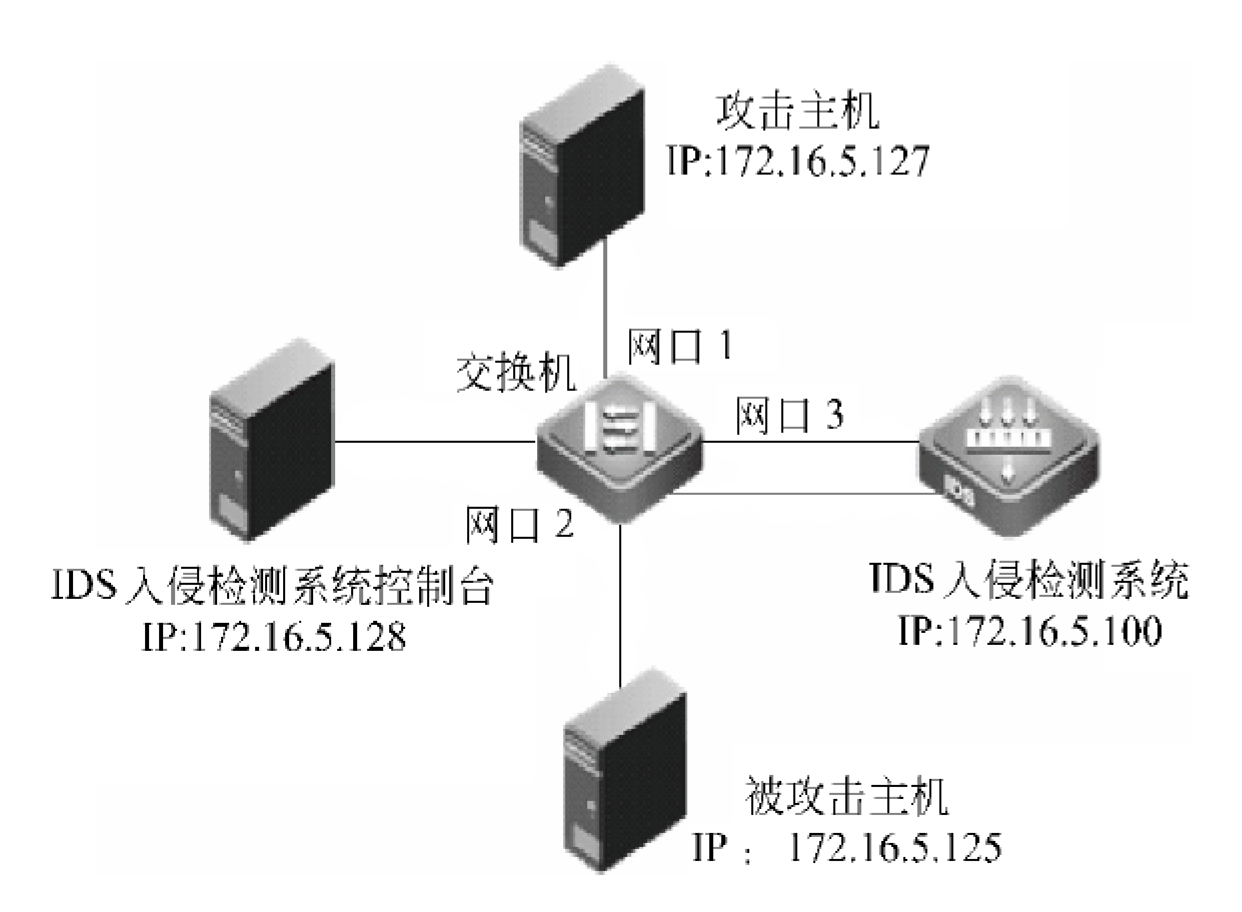



图 3-3　IDS 监听系统模型

- 检测黑客在攻击前的探测行为，预先给管理员发出警报；
- 报告计算机系统或网络中存在的安全威胁；
- 提供攻击的信息，帮助管理员诊断网络中存在的安全弱点，利于修补；
- 在大型、复杂网络中布置入侵检测系统，提高网络安全管理质量。

IDS 的运行方式有两种：一种是在目标主机上运行以监测其本身的通信信息；另一种是在一台单独的机器上运行以监测所有网络设备的通信信息，例如 Hub、路由器。当有某个事件与一个已知攻击的信号相匹配时，多数 IDS 都会警报。一个基于异常的 IDS 会构造一个当时活动的主机或网络的大致轮廓，当有一个在这个轮廓以外的事件发生时，IDS 就会告警。在 IDS 运行过程中，和以下几个关键字有关。

- 攻击(attacks)

攻击可以定义为试图渗透系统或者绕过系统安全策略而获取信息、更改信息、中断目标网络或者系统的正常运行的活动。

- 警报(alerts)

警报是 IDS 向系统操作员发出的有入侵正在发生或者正在尝试的消息。一旦侦测到入侵，IDS 会以各种方式向分析员发出警报。如果控制台在本地，IDS 警报通常会显示在监视器上。IDS 还可以通过声音报警(但在繁忙的 IDS 上建议关闭声音)。通过厂商的通信手段可以将警报发送到远程控制台，除此之外，还可以利用 SNMP 协议(安全性有待考虑)、E-mail、SMS/Pager 或者这几种方式的组合进行报警。

- 异常(anomaly)

大多 IDS 在检测到与已知攻击特征匹配的事件时就会发出警报，而基于异常的 IDS 会用一段时间建立一个主机或者网络活动的轮廓。在这个轮廓之外的事件也会发出 IDS 警报，也就是说，当有人进行以前从没有过的活动，IDS 就会发出警报。例如一个用户突然获得管理员权限(或者 root 权限)。一些厂商把这种方法称为启发式 IDS，但是真正的启发式 IDS 比这种方法有更高的智能性。

IDS 处理网络上数据信息的过程分为数据采集阶段、数据处理及过滤阶段、入侵分析及检测阶段、报告以及响应阶段 4 个阶段。

数据采集阶段是数据审核阶段，在入侵检测系统收集目标系统中，引擎提供主机通信数据包和系统使用等数据信息。入侵检测的第一步是数据信息收集，收集数据内容包括系统、网络、数据及用户活动的状态和行为。由放置在不同网段的传感器或不同主机的代理来收集信息，包括系统和网络日志文件、网络流量、非正常的目录和文件改变、非正常的程序执行。

而数据处理及过滤阶段则是对采集到的数据进行分析和处理，收集到的有关系统、网络、数据及用户活动的状态和行为等信息，送到检测引擎，检测引擎驻留在传感器中，一般通过 3 种技术手段进行分析：模式匹配、统计分析和完整性分析。当检测到某种误用模式时，产生一个警告并发送给控制台。

最后是报告以及响应阶段，通过控制台按照警告产生预先定义的响应而采取相应措施，可以重新配置路由器或防火墙、终止进程、切断连接、改变文件属性，也可以只是简单的警告。

通过分析上一阶段提供的数据、分析及检测入侵阶段来判断是否发生入侵，这一阶段是整个入侵检测系统的核心执行阶段。最后到了报告及响应阶段，针对上一个阶段进行的判断做出响应。如果通过数据来分析，判断网络中可能发生了入侵行为，系统将根据网络管理员事先配置的安全措施，对其采取相应的响应手段。此外也可以通过提示信息，通知网络管理人员网络发生了入侵，以便于采取措施。

## 3.4　入侵检测系统类型

入侵检测系统是从计算机网络系统中的若干关键点来收集信息，并分析这些信息，检查网络中是否有违反安全策略的行为或遭到袭击的迹象。入侵检测被认为是防火墙之后的第二道安全闸门。入侵检测通过对入侵行为的过程与特征进行研究，使安全系统对入侵事件和入侵过程做出实时响应。一般来讲，入侵检测系统按其输入数据的来源来看，可以分为 3 类：

### 1. 基于主机的入侵检测系统(HIDS)

基于主机的入侵检测系统输入数据来源于系统的审计日志，一般只能检测该主机上发生的入侵。基于主机的入侵检测产品通常是安装在被重点检测的主机之上，主要是对该主机的网络实时连接以及系统审计日志进行智能分析和判断。如果主体活动十分可疑(特征或违反统计规律)，入侵检测系统就会采取相应的措施。

基于主机的 IDS 对多种来源的系统和事件日志进行监控，将会发现可疑活动。基于主机的 IDS 也叫做主机 IDS，最适合于检测那些可以信赖的内部人员的误用以及已经避开了传统的检测方法而渗透到网络中的活动。除了完成类似事件日志阅读器的功能，主机 IDS 还对“事件/日志/时间”进行签名分析。在很多产品中还包含了启发式功能。因为主机 IDS 几乎是实时工作的，系统的错误可以很快地检测出来，技术人员和安全人士都非常喜欢它。现在，基于主机的 IDS 指基于服务器/工作站主机的所有类型的入侵检测系统。

基于主机的入侵检测系统的优点如下：

- 主机入侵检测系统对分析“可能的攻击行为”非常有用。
- 主机入侵检测系统在通常情况下比网络入侵检测系统误报率要低。
- 主机入侵检测系统可以部署在那些不需要广泛的入侵检测、传感器与控制台之间。

基于主机的入侵检测系统的弱点如下：

- 主机入侵检测系统安装在需要保护的设备上。
- 主机入侵检测系统的另一个问题是它依赖于服务器固有的日志与监视能力。
- 全面部署主机入侵检测系统代价较大，在企业中很难将所有主机用主机入侵检测系统保护，只能选择部分主机保护。那些未安装主机入侵检测系统的机器将成为保护的盲点，入侵者可利用这些机器达到攻击目标。
- 主机入侵检测系统除了监测自身的主机以外，根本不监测网络上的情况。

### 2. 基于网络的入侵检测系统（NIDS）

基于网络的入侵检测系统放置在比较重要的网段内，不停地监视网段中的各种数据包，输入数据来源于网络的信息流，能够检测该网段上发生的网络入侵。基于网络的入侵检测产品（NIDS）放置在比较重要的网段内，不停地监视网段中的各种数据包。

网络入侵检测系统的优点如下：

- 网络入侵检测系统能够检测来自网络的攻击，能够检测到未授权的非法访问。
- 网络入侵检测系统不需要改变服务器等主机配置，不需要在系统主机中安装额外软件，从而不影响这些主机的 CPU、I/O 盘等资源使用，也不会影响系统的性能。
- 由于网络入侵检测系统不像路由器、防火墙等关键设备那样工作，它不会成为系统中关键路径。网络入侵检测系统发生故障不会影响正常业务运行。部署一个网络入侵检测系统风险比主机入侵检测系统风险少得多。
- 网络入侵检测系统近年有向专业设备发展的趋势，安装这样的入侵检测系统非常方便，只需将定制设备接上电源，做一些配置，再将其连到网络上即可。

网络入侵检测系统的弱点如下：

- 网络入侵检测系统只检查它直接连接网段的通信，不能检测在不同网段的网络包。
- 网络入侵检测系统为了性能目标通常采用特征检测的方法，检测出普通的一些攻击，而很难实现一些复杂、需要大量计算与分析时间的攻击检测。
- 网络入侵检测系统可能会将大量的数据传回分析系统中。
- 网络入侵检测系统处理加密的会话过程比较困难，目前通过加密通道的攻击还不多，但随着 IPv6 的普及，这个问题会越来越突出。

### 3. 分布式入侵检测系统

采用上述两种数据来源的分布式入侵检测系统，能够同时分析来自主机系统审计日志和网络数据流的入侵检测系统，一般为分布式结构，由多个部件组成。

## 3.5 入侵检测系统设备介绍

IDS产品有软件和硬件两种，下面介绍的是IDS的硬件产品。

现在的IDS做成了硬件放到机架上，而不是安装在现有的操作系统中，这样很容易就可以把IDS嵌入网络。一个入侵检测产品通常由两部分组成：传感器(Sensor)和控制台(Console)。传感器负责采集数据(如网络包、系统日志等)、分析数据并生成安全事件。控制台主要起到中央管理的作用，商品化的产品通常提供图形界面的控制台，这些控制台基本上都支持Windows NT平台。

IDS设备的控制端口通常为Console端口，IDS的初始配置也是通过控制端口(Console)与PC(通常是便于移动的笔记本电脑)的串口(RS-232)连接，再通过Windows系统自带的超级终端(HyperTerminal)程序进行选项配置，如图3-4所示。




图3-4 IDS设备配置端口

## 3.6 入侵检测系统设备性能指标

对于IDS，用户会关注每秒能处理的网络数据流量、每秒能监控的网络连接数等指标。但除了基本的硬件性质指标外，其实还有一些不为一般用户了解的指标也很重要，例如每秒抓包数、每秒能够处理的事件数等。

### 1. 每秒数据流量(Mbps或Gbps)

每秒数据流量是指网络上每秒通过某节点的数据量。这个指标是反映网络入侵检测系统性能的重要指标，一般由Mbps来衡量。例如10Mbps、100Mbps和1Gbps。

网络入侵检测系统的基本工作原理是嗅探(Sniffer)，它通过将网卡设置为混杂模式，使得网卡可以接收网络接口上的所有数据。如果每秒数据流量超过网络传感器的处理能力，基于网络的入侵检测系统NIDS就可能会丢包，从而不能正常检测攻击。但是NIDS是否会丢包，不仅取决于每秒数据流量，还取决于每秒抓包数。

### 2 每秒抓包数(pps)

每秒抓包数是反映网络入侵检测系统性能的最重要的指标。因为系统不停地从网络上抓包，对数据包作分析和处理，查找其中的入侵和误用模式。所以，每秒所能处理的数据包的多少，反映了系统的性能。业界不熟悉入侵检测系统的人往往把每秒网络流量作为判断网络入侵检测系统的决定性指标，这种想法是错误的。

每秒网络流量等于每秒抓包数乘以网络数据包的平均大小。网络数据包的平均大小差异很大,因此在相同抓包率的情况下,每秒网络流量的差异也会很大。例如,网络数据包的平均大小为1024字节左右,系统的性能能够支持10 000pps的每秒抓包数,那么系统每秒能够处理的数据流量可达到78Mbps,当数据流量超过78Mbps时,会因为系统处理不过来而出现丢包现象;如果网络数据包的平均大小为512字节左右,在10 000pps的每秒抓包数的性能情况下,系统每秒能够处理的数据流量可达到40Mbps,当数据流量超过40Mbps时,就会因为系统处理不过来而出现丢包现象。

在相同的流量情况下,数据包越小,处理的难度越大。小包处理能力,也是反映防火墙性能的主要指标。

#### 3. 每秒能监控的网络连接数

网络入侵检测系统不仅要对单个的数据包进行检测,还要将相同网络连接的数据包组合起来进行分析。网络连接的跟踪能力和数据包的重组能力是网络入侵检测系统进行协议分析、应用层入侵分析的基础。这种分析延伸出很多网络入侵检测系统的功能,例如,检测利用HTTP协议的攻击、敏感内容检测、邮件检测、Telnet会话的记录与回放、硬盘共享的监控等。

#### 4. 每秒能够处理的事件数

网络入侵检测系统检测到网络攻击和可疑事件后,会生成安全事件或称报警事件,并将事件记录在事件日志中。每秒能够处理的事件数,反映了检测分析引擎的处理能力和事件日志记录的后端处理能力。有的厂商将反映这两种处理能力的指标分开,称为事件处理引擎的性能参数和报警事件记录的性能参数。

大多数网络入侵检测系统报警事件记录的性能参数小于事件处理引擎的性能参数,主要是Client/Server结构的网络入侵检测系统,引入了网络通信的性能瓶颈。这种情况将导致事件的丢失,或者控制台响应缓慢。

## 3.7 入侵检测产品选择要点

防火墙看起来好像可以满足系统管理员的一切需求。然而,随着攻击行为和产品自身问题的增多,IDS由于能够在防火墙内部监测非法的活动变得越来越重要。新的技术同样给防火墙带来了严重的威胁。

当组建安全网络需要选择入侵检测系统时,要考虑的要点如下:

#### 1. 系统的价格

当然,价格是必须考虑的要点,不过,性能价格比,以及要保护系统的价值是更重要的因素。

#### 2. 特征库升级与维护的费用

像反病毒软件一样,入侵检测的特征库需要不断更新才能检测出新出现的攻击方法。

### 3. 网络入侵检测系统的最大可处理流量

要分析网络入侵检测系统所部署的网络环境，如果在 512K 或 2M 专线上部署网络入侵检测系统，则不需要高速的入侵检测引擎，而在负荷较高的环境中，性能是一个非常重要的指标。

### 4. 该产品容易被躲避

有一些常用的躲开入侵检测的方法，如分片、TTL 欺骗、异常 TCP 分段、慢扫描、协同攻击等。

### 5. 产品的可伸缩性

系统支持的传感器数目、最大数据库大小、传感器与控制台之间通信带宽和对审计日志溢出的处理。

### 6. 运行与维护系统的开销

产品报表结构、处理误报的方便程度、事件与日志查询的方便程度以及使用该系统所需的技术人员的数量。

### 7. 产品支持的入侵特征数

不同厂商对检测特征库大小的计算方法不一样。

### 8. 产品有哪些响应方法

要从本地、远程等多个角度考察。自动更改防火墙配置是一个很“酷”的功能，但是自动配置防火墙是一个极为危险的举动。

### 9. 是否通过了国家权威机构的评测

主要的权威测评机构有：国家信息安全测评认证中心、公安部计算机信息系统安全产品质量监督检验中心。

# 第 4 章 入侵检测系统实践技术

## 4.1 RG-IDS 账户管理

### 【实验名称】

RG-IDS 账户管理。

### 【实验目的】

掌握配置 RG-IDS 管理账户的方法。

### 【背景描述】

某企业部署了一台 RG-IDS 进行攻击检测，现在需要对 RG-IDS 进行管理。

### 【需求分析】

通过添加管理员账户，可以对 RG-IDS 进行配置管理操作。

### 【实验拓扑】

如图 4-1 所示的网络拓扑，是企业为了提高网络的安全，部署一台 RG-IDS 进行攻击检测，希望能够对 RG-IDS 进行管理，通过添加管理员账户，可以对 RG-IDS 进行配置管理操作，来实现网络的安全防范功能。

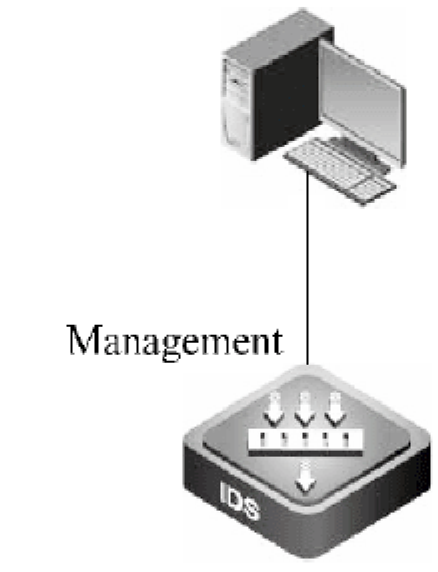



图 4-1　RG-IDS 攻击检测网络规划拓扑图

### 【实验设备】

| | |
|---|---|
| PC | 1 台 |
| RG-IDS Sensor | 1 台 |
| 直连线 | 1 条 |

### 【预备知识】

- RG-IDS 基本配置。

### 【实验原理】

用户管理承担着系统认证中心的角色。用户登录时认证中心对用户名、密码进行认

证,如果有绑定设置则根据其绑定方式(静态绑定、动态绑定)对用户作绑定处理。此外,在认证登录用户时,如果某个用户从相同的 IP(隐含的动态绑定)重复多次登录尝试,则将该用户视为可疑用户,认证中心会将该用户锁定,同时发送审计事件通知用户管理员(触发锁定的登录尝试次数用户管理员可以在创建时指定)。

用户管理还可以添加、删除用户和修改用户信息,并且可以为不同的用户分配权限。不同角色的用户具有不同的权限,每一位用户都不能越权操作。

## 【实验步骤】

### 1. 用户管理员登录

使用默认的 Admin 账号登录系统(默认安装时用户 Admin 的密码为 Admin,建议用户管理员第一次登录后修改该密码),如图 4-2 所示。




图 4-2　管理员用户账号登录

登录成功后,用户管理界面如图 4-3 所示。

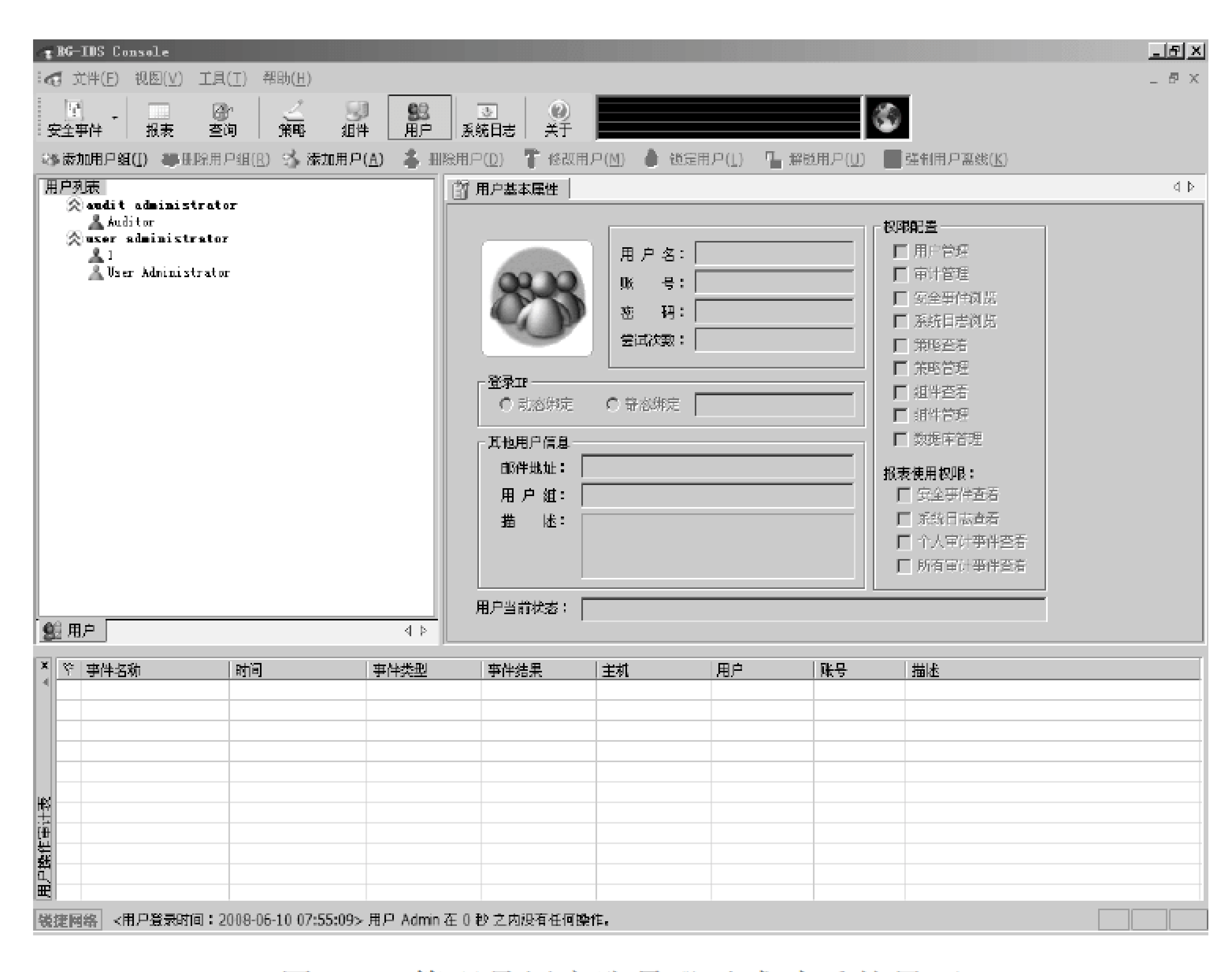


图 4-3　管理员用户账号登录成功后的界面

## 2 用户查看

查看用户列表中各用户的状态，如图 4-4 所示。

各个图标表示的用户状态如表 4-1 所示。

表 4-1　用户状态信息

| 图标 | 状　态 | 描　　述 |
|---|---|---|
| | 在线状态 | 在线状态的图标为绿色 |
| | 离线状态 | 离线状态的图标为暗红色 |
| | 锁定状态 | 用户被管理员锁定图标为暗红色并且标有禁止标记 |

双击某个用户查看其详细信息，如图 4-5 所示。

用户列表
audit administrator
Auditor
user administrator
1
User Administrator

图 4-4　查看用户列表




图 4-5　查看用户的详细信息

系统管理员登录管理平台的默认用户是 Admin 和 Audit。Admin 用户的默认密码是 Admin，Audit 用户的默认密码为 Audit。系统默认安装用户为 Admin 和 Audit，分别为用户管理和审计管理权限。Admin 不能修改 Audit 的密码。其他用户的密码由管理员分配。

## 3 新建一个用户

单击“添加用户(A)”按钮，在“用户属性配置”对话框中添加该用户的基本信息以及给该用户分配权限，如图 4-6 所示。

权限配置中各字段的含义如表 4-2 所示。

报表使用权限中各字段的含义如表 4-3 所示。

单击“确定”按钮，该用户已添加成功，如图 4-7 所示。

## 4 验证该用户

用新建的用户登录系统，如图 4-8 所示。




图 4-6　新建一个用户

**表 4-2　权限配置各字段含义**

| 字段 | 描　　述 |
|---|---|
| 用户管理 | 勾选此复选框，用户具有创建、删除用户和组，编辑用户基本信息，拥有锁定用户和解除用户锁定以及注销用户的权限 |
| 审计管理 | 勾选此复选框，用户具有通过用户操作审计表查看其他用户的操作审计结果的权限 |
| 安全事件浏览 | 勾选此复选框，用户有权限查看或使用事件分析器对 IDS 告警事件进行在线浏览和分析 |
| 系统日志浏览 | 勾选此复选框，用户有权查看系统日志，监视各个组件的状态 |
| 策略查看 | 勾选此复选框，用户有权查看策略集的配置方式和帮助信息，但是没有权限修改、派生、删除任何策略或策略集 |
| 策略管理 | 勾选此复选框，用户有权编辑和修改策略(应用策略属于组件管理) |
| 组件查看 | 勾选此复选框，用户有权查看组件的配置、属性和状态，但是没有权限增加、删除或修改任何组件及其属性 |
| 组件管理 | 勾选此复选框，用户有权添加、修改、删除以及操作组件的类型、数量和范围 |
| 数据库管理 | 勾选此复选框，用户具有对数据库的访问和控制权限，例如浏览、备份、删除和使用 Report 组件 |

**表 4-3　报表使用权限各字段含义**

| 字　　段 | 描　　述 |
|---|---|
| 安全事件查看 | 勾选此复选框，用户有权在报表中查看某种条件下安全事件的汇总 |
| 系统日志查看 | 勾选此复选框，用户有权在报表中查看某种条件下系统日志的汇总 |
| 个人审计事件查看 | 勾选此复选框，该用户有权在报表中查看某种条件下该人的操作审计事件记录的汇总 |
| 所有审计事件查看 | 勾选此复选框，用户有权在报表中查看某种条件下所有人的操作审计事件记录的汇总 |

用户列表
audit administrator
Auditor
user administrator
1
test
User Administrator

图 4-7　添加用户成功




图 4-8　用新建的用户登录系统

登录成功后的界面如图 4-9 所示。

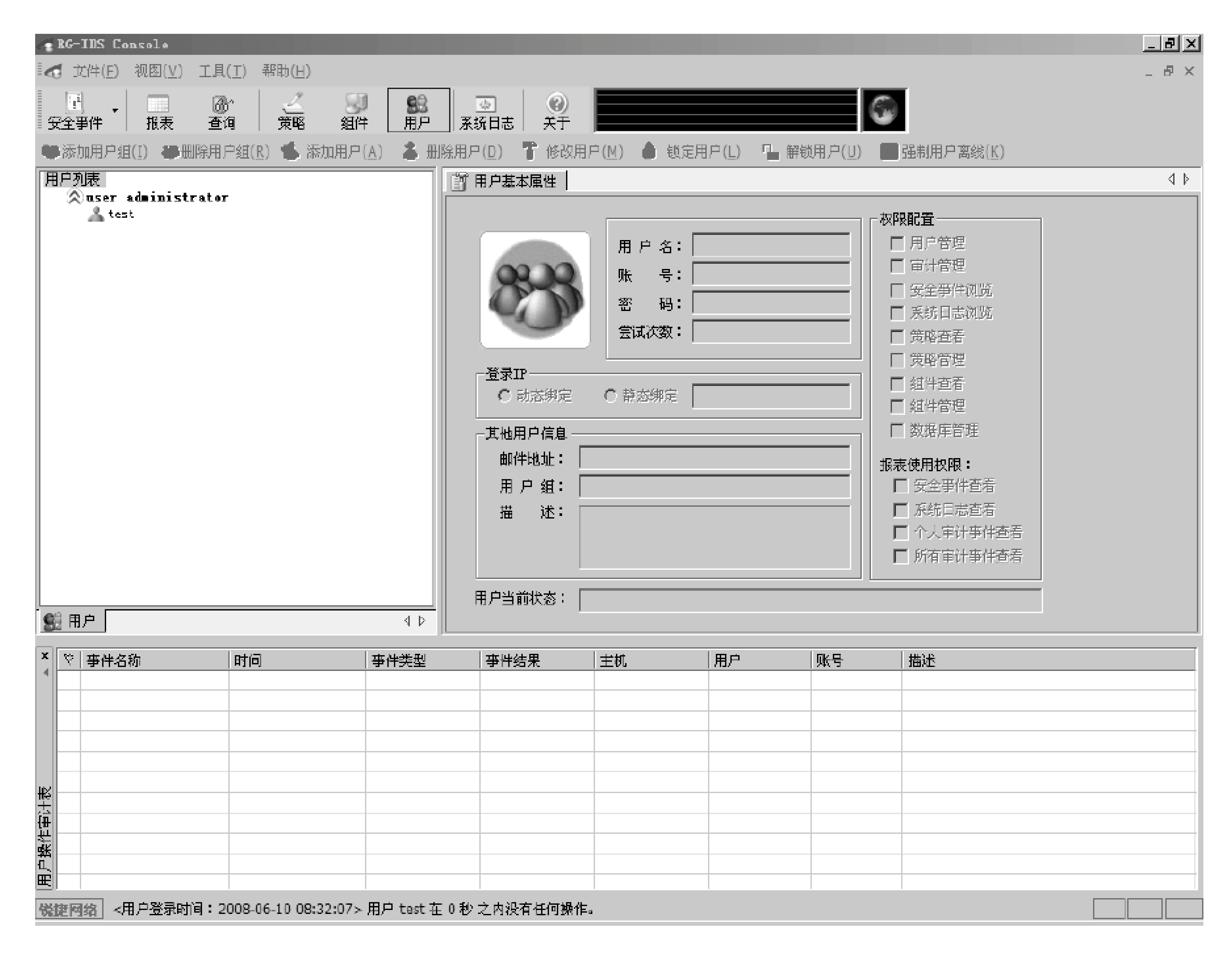



图 4-9　登录成功后的界面

### 5. 验证管理权限

用户可以查看本系统的策略，如图 4-10 所示。

切换用户，改用 Admin 登录，并在“用户列表”区域双击该用户，如图 4-11 所示。

在“权限配置”选项组中把该用户的“策略查看”、“策略管理”复选框取消勾选，如图 4-12 所示。

再次验证该用户的权限。切换到 test 用户，该用户已无法查看本系统的策略，如图 4-13 所示。

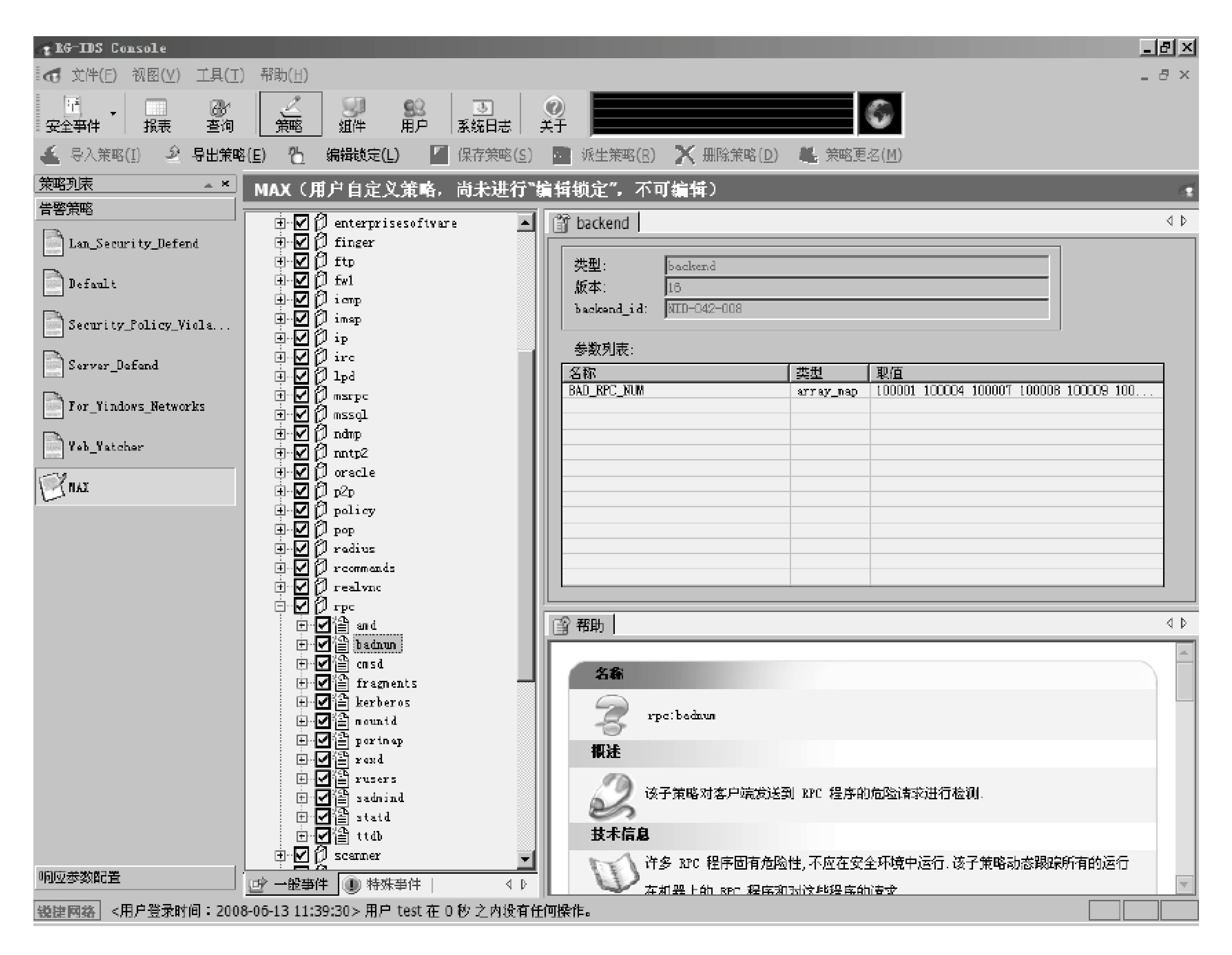



图 4-10　查看本系统的策略

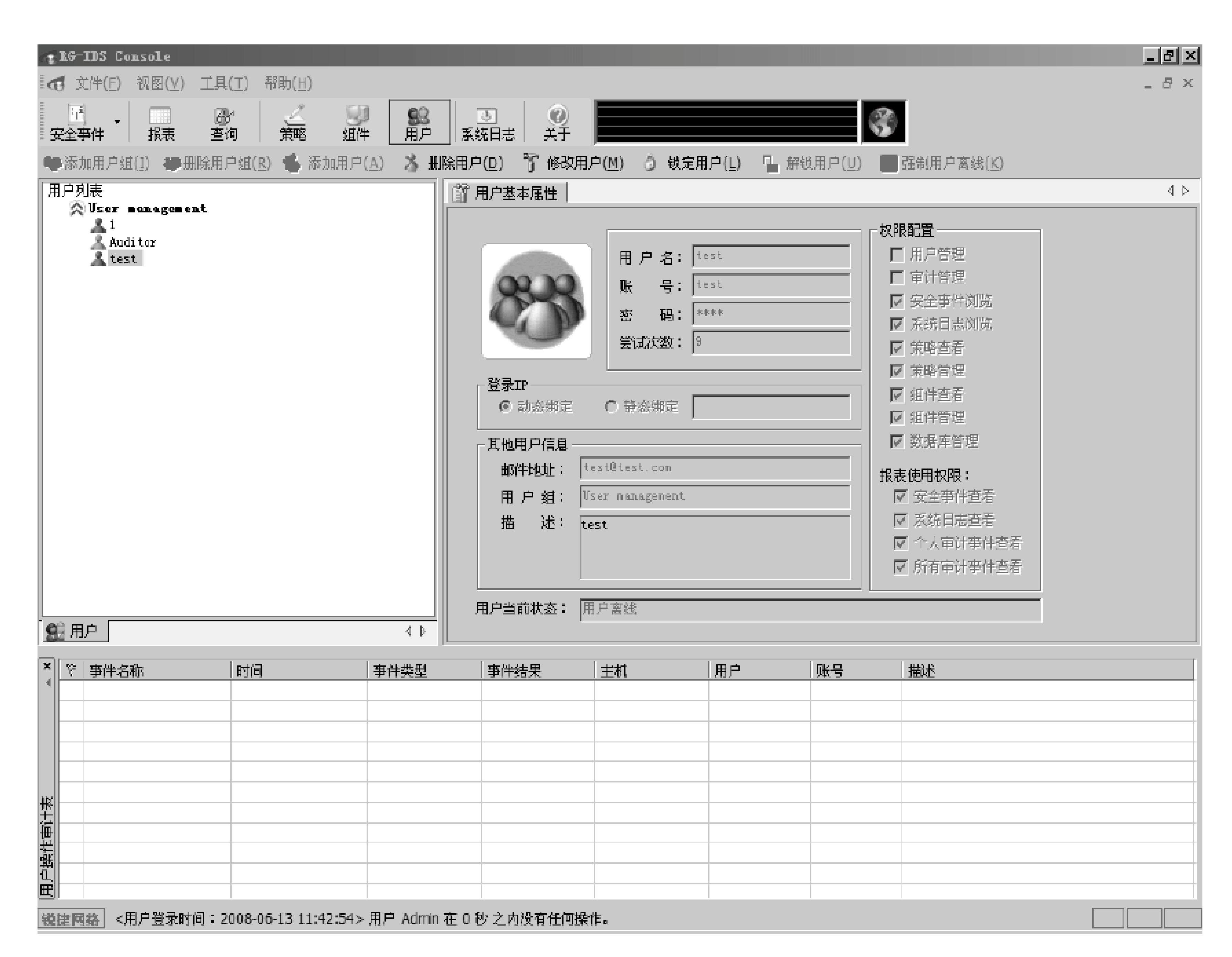



图 4-11　使用 Admin 登录并查看用户




图 4-12　取消用户权限

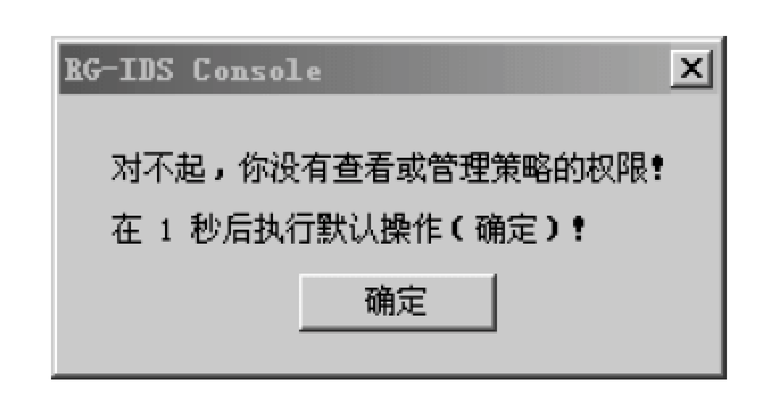



图 4-13　验证该用户的权限

## 4.2　RG-IDS 组件管理

### 【实验名称】

RG-IDS 组件管理。

### 【实验目的】

掌握 RG-IDS 组件的添加方式。

### 【背景描述】

某用户根据实际网络环境进行 IDS 的配置管理。

### 【需求分析】

某企业需要部署一台 RG-IDS 进行攻击检测，在将 RG-IDS 部署到网络中前，需要对 RG-IDS 进行初始化配置，并安装相关组件。

## 【实验拓扑】

如图 4-14 所示的网络拓扑，是企业为了提高网络的安全，部署一台 RG-IDS 进行攻击检测，在部署 RG-IDS 之前，希望能够对 RG-IDS 进行初始化配置的网络拓扑规划图，以实现网络的安全防范功能。

RG-IDS 控制台、时间收集器、日志服务器

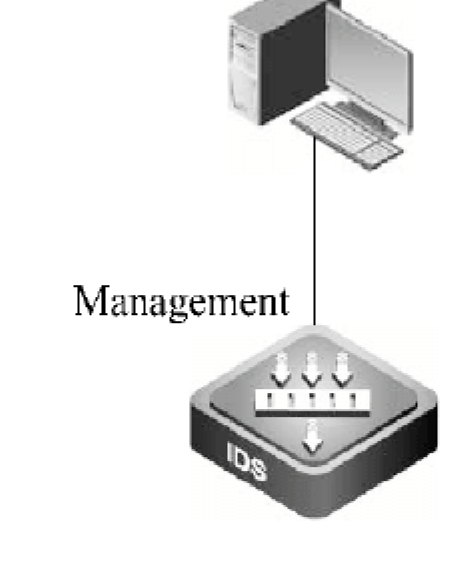



图 4-14 RG-IDS 初始化配置网络规划拓扑图

## 【实验设备】

PC 1 台

RG-IDS Sensor 1 台

直连线 1 条

## 【预备知识】

RG-IDS 基本配置步骤。

## 【实验原理】

通过 RG-IDS 控制台，添加多个组件，实现对 RG-IDS 的管理、接收告警事件等。

## 【实验步骤】

### 1. 初始化 LogServer

在安装 LogServer 的过程中需要进行数据库初始化配置，如图 4-15 所示。

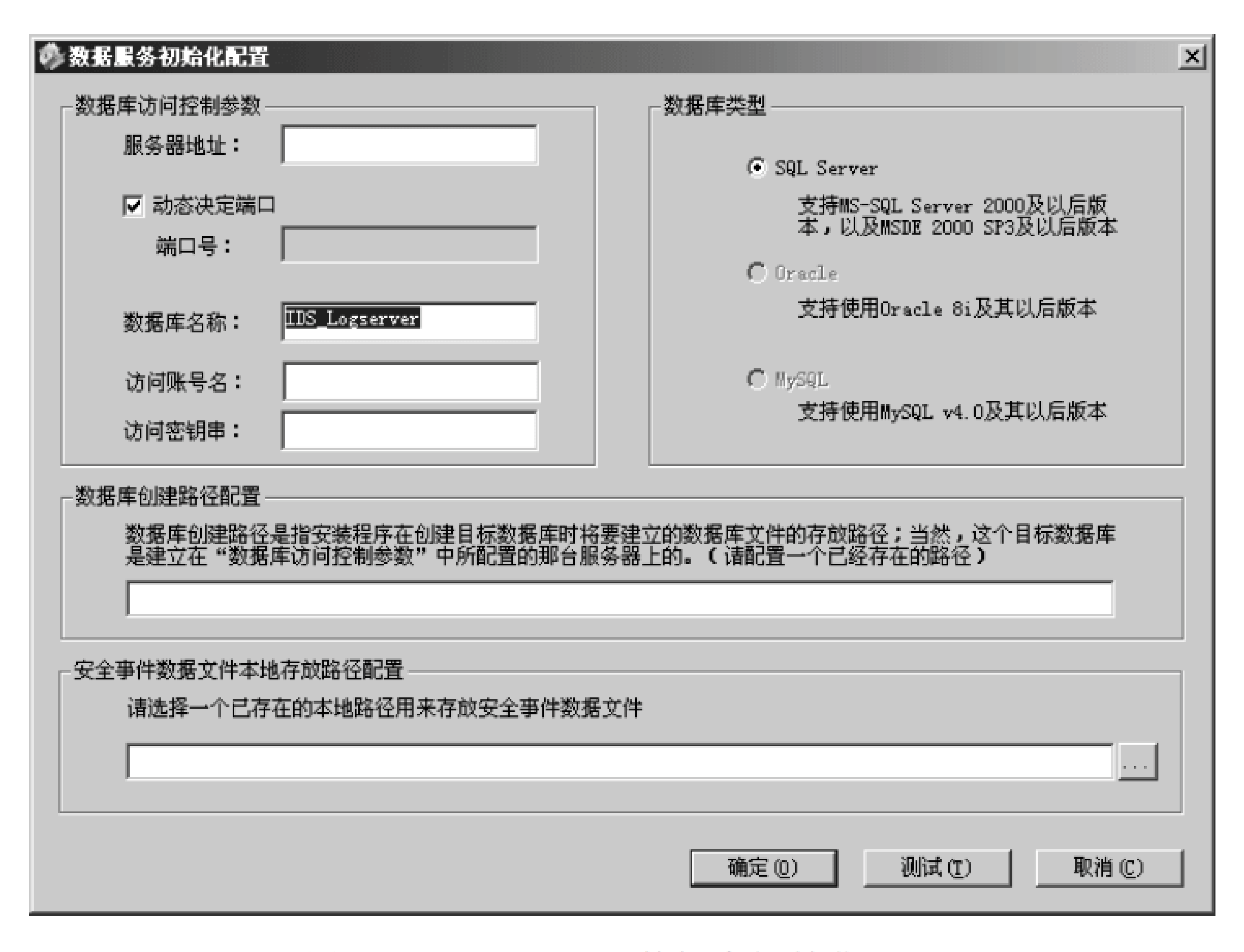



图 4-15 LogServer 数据库初始化配置

可以在此时对 LogServer 进行配置，也可单击“跳过”按钮，日后需要使用该模块时依次选择“开始”→“程序”→“锐捷入侵检测系统”→“锐捷入侵检测系统(网络)”→“RG-IDS

数据服务安装”选项进行初始配置(注：本步骤的前提是已安装 Microsoft SQL Server 或 MSDE 并有数据库管理员权限)。

## 2 根据实际情况配置 LogServer

数据服务初始化配置如图 4-16 所示。

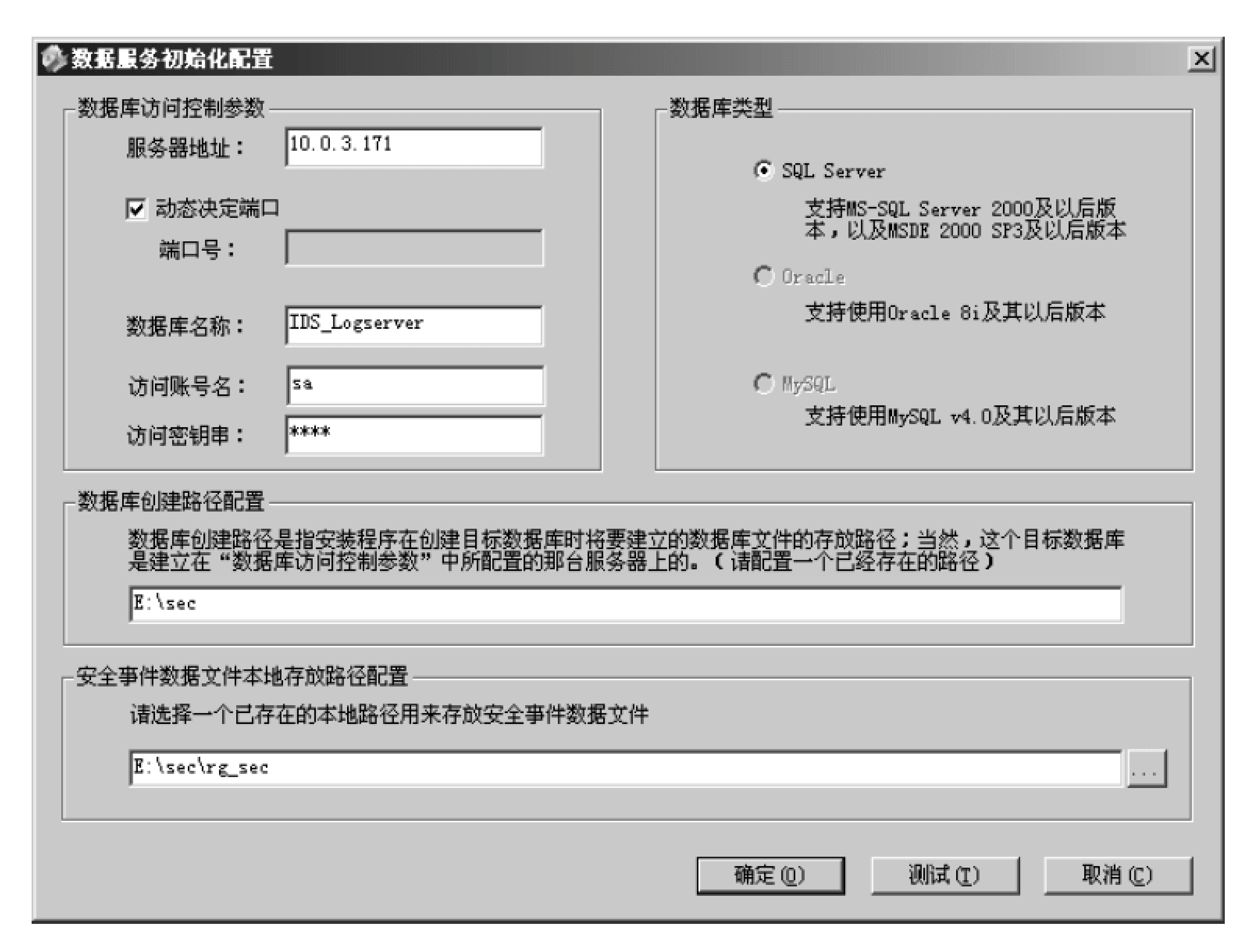



图 4-16　配置 LogServer 初始化

完成参数设置后请单击“测试”按钮，若一切无误会弹出以下提示框，如图 4-17 所示。

单击“确定”按钮返回到“数据服务初始化配置”对话框，再次单击“确定”按钮，稍等片刻会出现“数据库初创建成功！”的提示框，如图 4-18 所示。

## 3. 添加 LogServer

登录系统，在 EC 处单击 添加组件(A) 按钮，在弹出的“添加组件”对话框的下拉菜单中选择 LogServer 选项，如图 4-19 所示。




图 4-17　数据库初始化连接测试




图 4-18　数据库初创建成功




图 4-19　添加组件

在“LogServer 属性配置”对话框中填上需要添加的 LogServer 的相应信息，然后单击“确定”按钮，如图 4-20 所示。

返回到“组件管理”窗口，双击 LogServer，如图 4-21 所示。

打开“LogServer 配置属性”对话框，单击“容量检测”按钮，如图 4-22 所示。

添加成功，如图 4-23 所示。




图 4-20　添加的 LogServer 组件的相应信息




图 4-21　进入“组件管理”窗口




图 4-22　配置 LogServer 容量检测属性(1)




图 4-23　配置 LogServer 容量检测属性(2)

## 4. 添加传感器

在 EC 处单击“添加组件(A)”按钮,在弹出的“添加组件”对话框的下拉菜单中选择“传感器”选项,如图 4-24 所示。

在“传感器属性配置”对话框中填上需要添加的传感器的相应信息。然后单击“连接测试”按钮,如图 4-25 所示。

添加组件
请选择要添加的组件类型:
传感器
确定
取消

图 4-24　添加传感器

在弹出的连接测试成功提示框中单击“确定”按钮，如图 4-26 所示。




图 4-25　配置传感器属性(1)




图 4-26　连接测试信息

返回到“传感器属性配置”对话框中并单击“确定”按钮，如图 4-27 所示。

添加成功，如图 4-28 所示。




图 4-27　配置传感器属性(2)

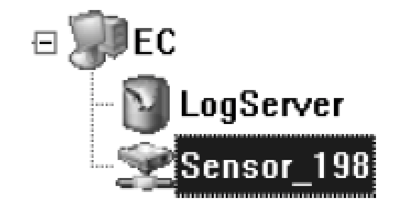



图 4-28　配置传感器属性信息

## 【注意事项】

- 如果添加组件提示超时，有可能是由个人防火墙的配置造成的，请正确配置防火墙。
- 当进行多个 IDS 的分布式部署时，可以使用相同的方法添加多个传感器组件，如图 4-29 所示。




图 4-29　在 IDS 分布式部署中添加多个传感器组件

## 4.3　RG-IDS 策略管理

### 【实验名称】

RG-IDS 策略管理。

### 【实验目的】

通过策略管理控制引擎监测的内容。

### 【背景描述】

某企业部署一台 RG-IDS 进行攻击检测，管理员希望根据不同网络环境定制相应的策略。

### 【需求分析】

需求：解决根据不同的网络环境定制相应策略的问题。

分析：用户根据网络实际运行情况自定义策略。

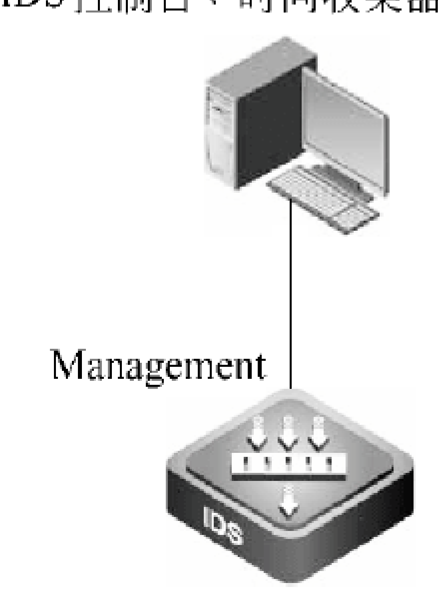



图 4-30　RG-IDS 策略管理网络拓扑图

### 【实验拓扑】

如图 4-30 所示的网络拓扑，是企业为了提高网

络的安全，部署一台 RG-IDS 进行攻击检测，在部署 RG-IDS 之前，管理员希望根据不同网络环境定制相应策略的网络拓扑规划图，以实现网络的安全防范功能。

## 【实验设备】

| | |
|---|---|
| PC | 3 台 |
| RG-IDS | 1 台 |
| 直连线 | 4 条 |
| 交换机 | 2 台(其中一台必须支持多对一的端口镜像配置) |

## 【预备知识】

RG-IDS 基本配置。

## 【实验原理】

传感器使用策略来控制其所监测的内容，并对监测到的事件做出响应。用户可以使用系统管理平台所附带的预定义策略，也可以从预定义策略派生新的策略。预定义策略分别侧重于用户所关心的各种层面，用户可以选择适合自己的预定义策略直接应用。考虑到用户的不同需求，系统管理平台提供了用户自定义策略的功能。用户可以从预定义策略派生新的策略并且对新策略进行编辑，用户还可对其关心的部分攻击签名进行微调，以便更符合用户的需要。

在策略管理中，用户需要配置安全事件的响应方式。这些响应方式包括 Console 显示、Write DB、SNMP Trap、E-mail、OPSEC 以及用户自定义响应。其中除 Console 显示和 Write DB 不需要配置外，其他响应方式均需要做相应的配置工作。

## 【实验步骤】

### 1. 策略编辑界面浏览

如图 4-31 所示，单击主界面上的“策略”按钮，切换到策略编辑器界面，策略编辑器的窗口分为 4 个区域。通过“策略编辑器”窗口，可以新建、派生、修改、删除、查看、导入和导出策略。

在告警策略模板区域中列出了当前可用的策略，其中包括系统的预定义策略和用户自定义策略。预定义策略不能更改，用户可以根据自身的网络情况选择某个预定义策略而派生出自定义策略并且进行调整。图标代表预定义策略，不能进行编辑，只能单独应用到传感器，可以派生出自定义策略。图标代表自定义策略，能进行编辑和操作。

系统自带 8 种针对不同环境配置的预定义策略，针对这些策略的详细说明，请参考《RG-IDS 用户操作和使用手册》。

### 2 派生新策略

在策略模板区域选中一个预定义策略 Attack-Detector，右键单击该策略，在弹出的

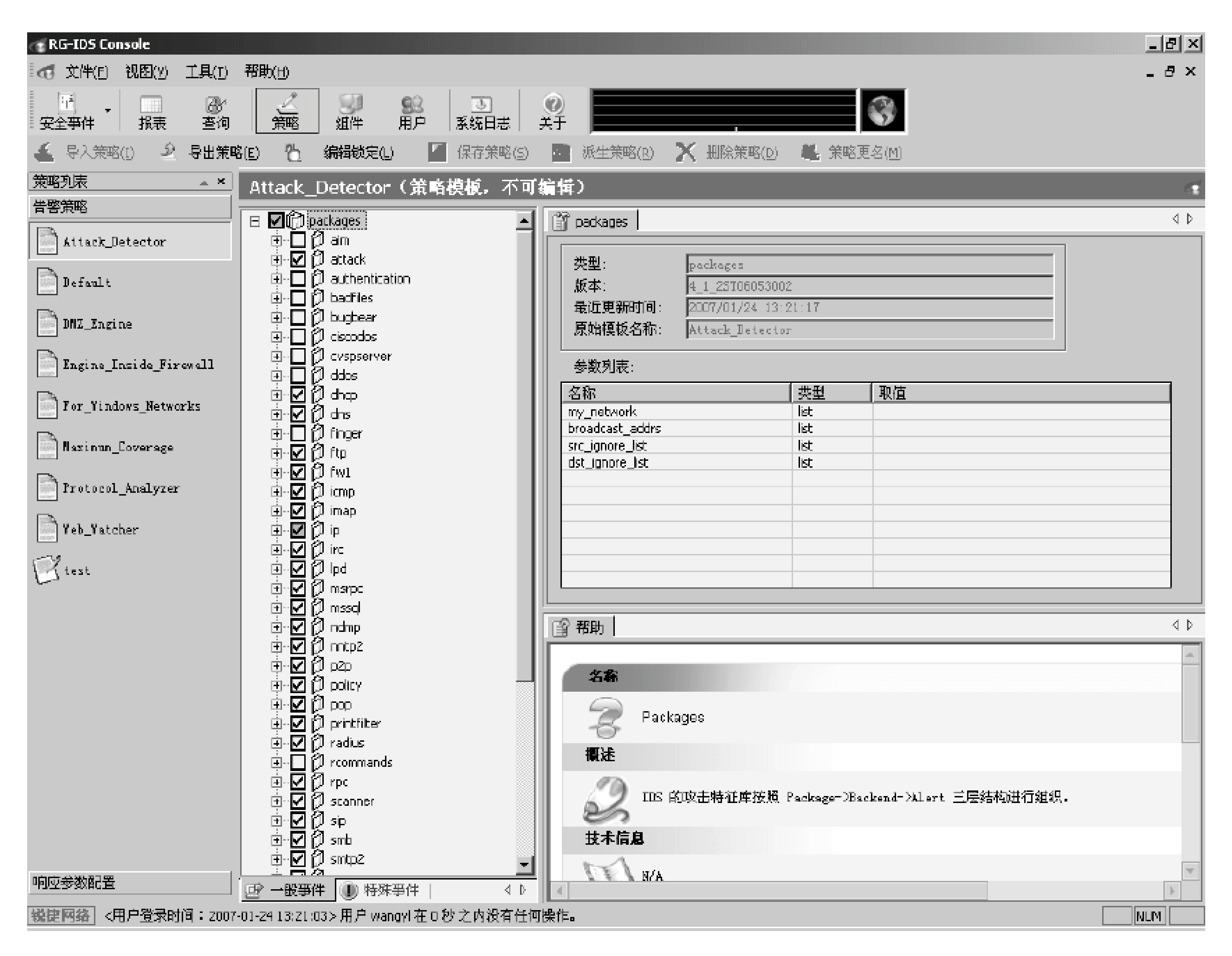



图 4-31　RG-IDS 策略编辑器界面

菜单中选择“派生策略”命令，如图 4-32 所示。

在弹出的对话框中输入新策略的名称，如图 4-33 所示。

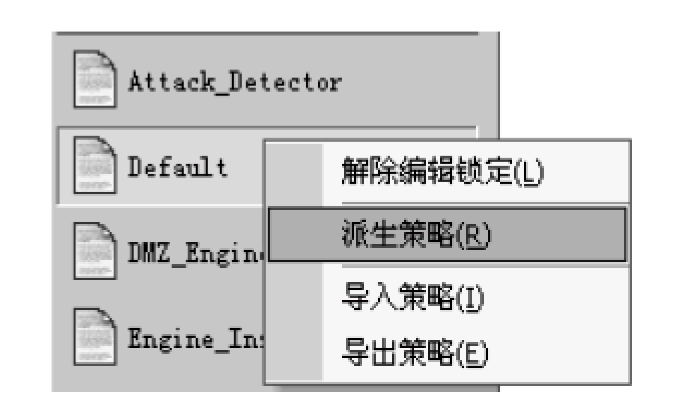



图 4-32　RG-IDS 策略管理派生新策略




图 4-33　输入新策略的名称

单击“确定”按钮，新策略显示在告警策略模板中。

## 3. 策略编辑

在策略中可以选择用户所关注的事件签名进行检测，编辑策略的步骤如下：

(1) 单击一个自定义策略。

(2) 单击“编辑锁定”按钮以确保其他人不能同时更改策略。

(3) 在攻击签名窗口展开攻击签名。

(4) “选中”或“取消选中”攻击签名。

(5) 为攻击签名选择响应方式。

(6) 单击“保存策略”按钮。

**注意：**不能编辑预定义策略。可以由预定义策略派生出一个新策略，然后对新策略进行调整。

### 4. 策略锁定和解除策略锁定

锁定策略时，在策略管理窗口单击“编辑锁定”按钮，策略管理窗口将被锁定。当多用户同时登录控制台时，当前用户可以编辑策略，其他用户不能修改。

解除策略锁定时，在策略管理窗口单击“解除锁定”按钮，编辑权限被释放，当多用户同时登录控制台时，允许其他用户编辑策略。

### 5. 导出策略

右键单击一个策略，在弹出的菜单中选择“导出策略”命令，如图 4-34 所示。

在弹出的窗口中选择导出策略的位置，如图 4-35 所示。

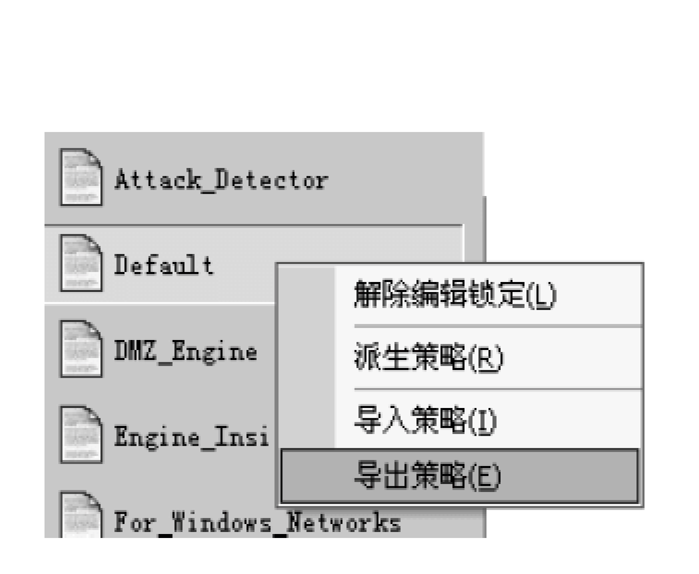



图 4-34　导出策略

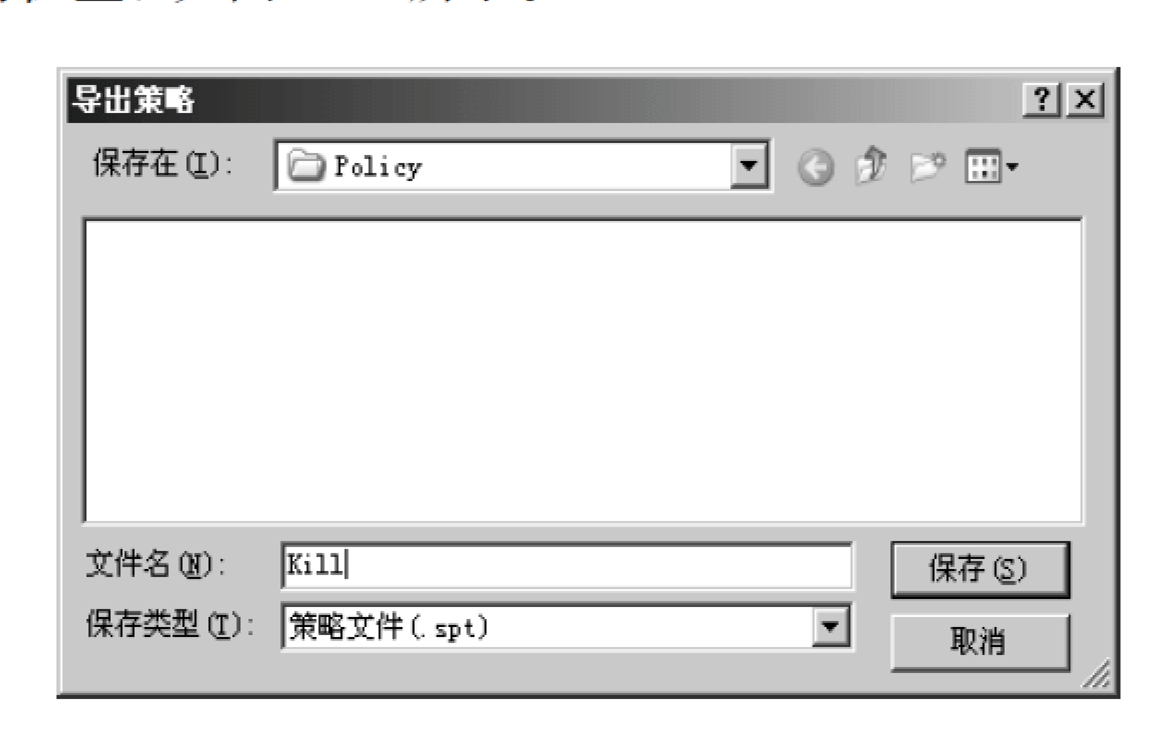



图 4-35　选择导出策略的位置

输入另存的文件名，单击“保存”按钮。

### 6. 导入策略

右键单击某个策略，在弹出的菜单中选择“导入策略”命令，如图 4-36 所示。

在弹出的窗口中选择导入策略的位置，如图 4-37 所示。

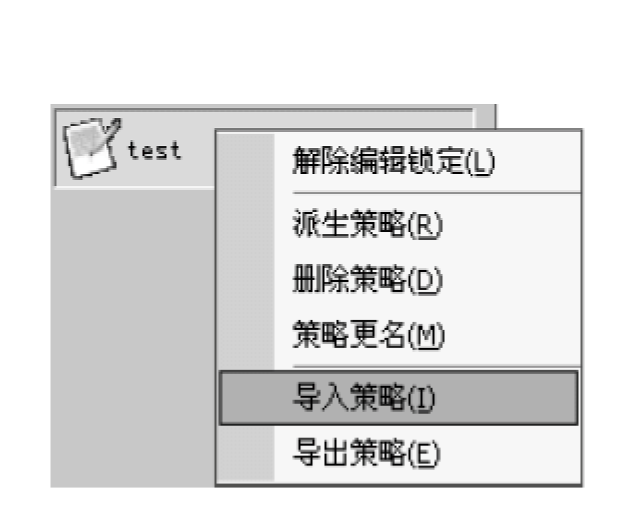



图 4-36　导入策略




图 4-37　选择导入策略的位置

选择导入的策略，单击“打开”按钮，如图 4-38 所示。

策略导入成功。

### 7. 策略应用

打开“组件”，在 EC 下面的“引擎”上单击右键，在弹出的菜单中选择“应用策略”命令，如图 4-39 所示。




图 4-38 选择导入的策略

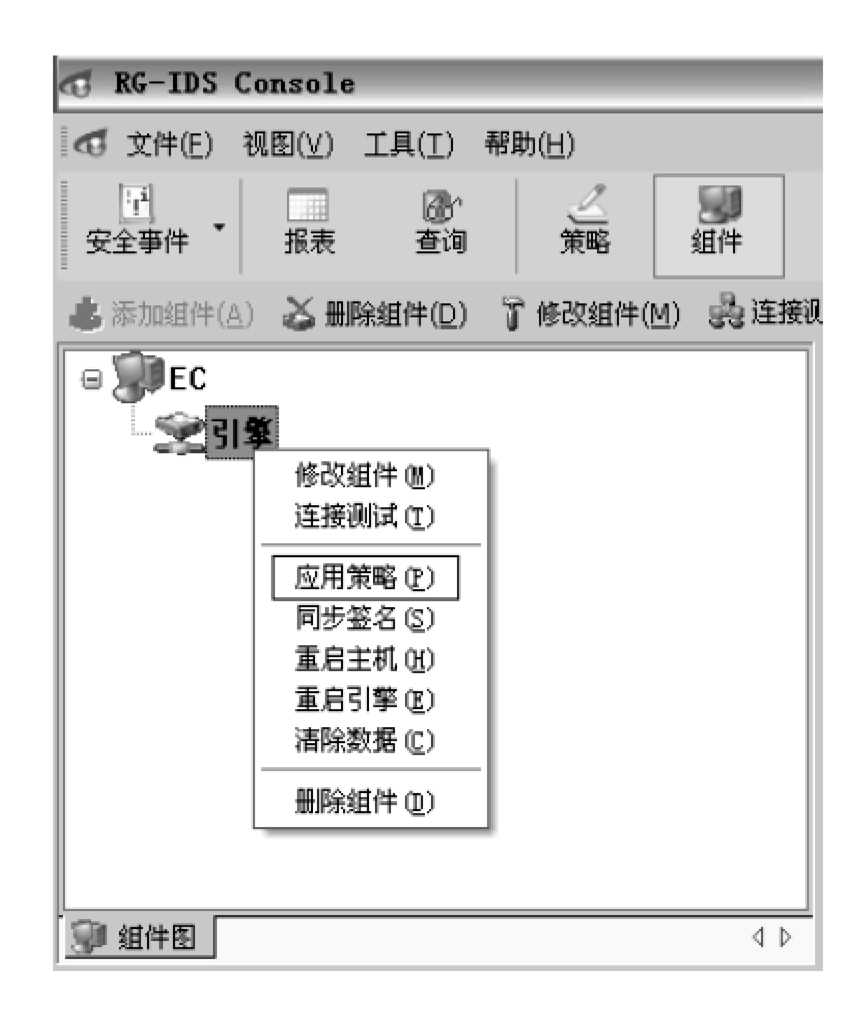



图 4-39 应用策略

在弹出的“应用策略”对话框中选择需要下发的策略，单击“应用”按钮，如图 4-40 所示。弹出“命令处理进度…”对话框，如图 4-41 所示，下发完毕后引擎会自动重启。




图 4-40 选择需要下发的策略

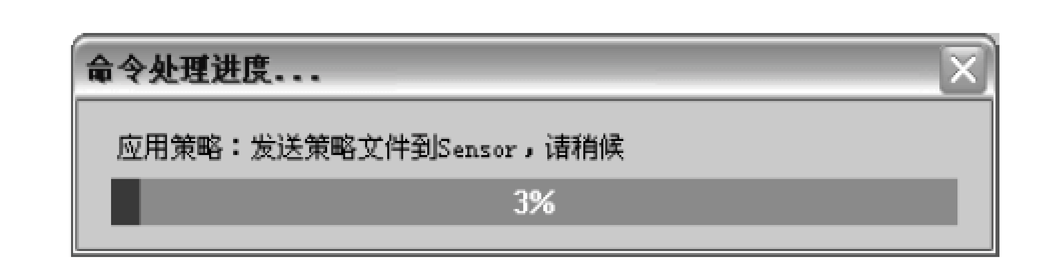



图 4-41 “命令处理进度…”对话框

## 【注意事项】

- 不能编辑预定义策略，可以由预定义策略派生出一个新策略，然后对新策略进行调整。
- 如果用户定义的策略不能编辑，请检查策略编辑是否已经锁定，并进行解锁。

# 4.4 配置交换机端口镜像

## 【实验名称】

配置交换机端口镜像。

## 【实验目的】

使用交换机的端口镜像功能分析网络中的特定流量。

## 【背景描述】

某企业网络管理员发现网络中有异常流量，需要对网络流量进行手动分析。

## 【需求分析】

对于网络中需要管理员进行手工分析的异常流量，需要将管理员 PC 配置成端口镜像机器，异常流量的数据包都镜像到管理员 PC，然后抓取数据包。

## 【实验拓扑】



图 4-42　配置交换机端口镜像网络拓扑图

如图 4-42 所示的网络拓扑，某企业网络管理员发现网络中有异常流量，需要对网络流量进行手动分析，为了提高网络的安全，需要将流量异常数据包通过镜像端口转发到管理员 PC，然后抓取数据包，实现网络的安全防范功能。

## 【实验设备】

交换机　　1 台
PC　　　　3 台

## 【预备知识】

- 交换机转发原理。
- 交换机基本配置。
- 端口镜像原理。

## 【实验原理】

交换机的端口镜像特性可以允许管理员对网络中的特定流量进行镜像分析，即在交换机上，对特定流量进行复制并发送到指定端口。

## 【实验步骤】

### 1. 定义需要镜像的特定流量

```
Switch# configure
Switch(config)# monitor session 1 source interface fastEthernet 0/1 both
```

### 2 配置镜像流量的流出端口

```
Switch(config)# monitor session 1 destination interface fastEthernet 0/2
```

### 3. 验证测试

将 PC1 接入 F0/1 接口,PC2 接入 F0/2 接口,PC1 与 PC2 之间可以互相 ping 通。

### 4. 验证测试

将 PC3 接入 F0/3 接口,且设置其 IP 地址为 192.168.1.3,并使用抓包软件进行抓包。在 PC1 上 ping PC2 的 IP 地址。

由于 PC1 到 PC2 的流量被交换机镜像到了 F0/3 端口,所以在 PC3 上使用抓包软件可以抓到 PC1 到 PC2 的网络流量,如图 4-43 所示。

| No. | Time | Source | Destination | Protocol | Info |
|---|---|---|---|---|---|
| 6 | 2.545877 | 192.168.1.1 | 192.168.1.2 | ICMP | Echo (ping) request |
| 7 | 2.545974 | 192.168.1.2 | 192.168.1.1 | ICMP | Echo (ping) reply |
| 8 | 3.546386 | 192.168.1.1 | 192.168.1.2 | ICMP | Echo (ping) request |
| 9 | 3.546502 | 192.168.1.2 | 192.168.1.1 | ICMP | Echo (ping) reply |
| 11 | 4.546342 | 192.168.1.1 | 192.168.1.2 | ICMP | Echo (ping) request |
| 12 | 4.546449 | 192.168.1.2 | 192.168.1.1 | ICMP | Echo (ping) reply |
| 14 | 5.546331 | 192.168.1.1 | 192.168.1.2 | ICMP | Echo (ping) request |
| 15 | 5.546447 | 192.168.1.2 | 192.168.1.1 | ICMP | Echo (ping) reply |

图 4-43　验证测试

## 【参考配置】

```
Switch# show running-config

Building configuration…
Current configuration: 611 bytes

!
version 1.0
!
hostname Switch
!
interface vlan 1
  no shutdown
!
monitor session 1 destination interface fastEthernet 0/2
monitor session 1 source interface fastEthernet 0/1 both
end
```

# 4.5　端口扫描攻击检测

## 【实验名称】

端口扫描攻击检测。

## 【实验目的】

RG-IDS 对端口扫描(port scan)攻击的检测。

## 【背景描述】

在校园网中服务器被外网用户扫描和探测，RG-IDS 部署在外网出口、DMZ 区、数据中心，检测外网和内网用户对 DMZ 服务器、数据中心区应用层的攻击，以及恶意扫描和探测行为的审计。

## 【需求分析】

需求：外网用户的恶意扫描探测，内网用户遭受病毒攻击后，会自动向外发送扫描，传播蠕虫等病毒，危害内网安全。

分析：通过 RG-IDS 端口扫描攻击的检测，初步识别攻击的源和目的，从而进行及时防御，将威胁降到最低，更好地保护学校网络的安全。

## 【实验拓扑】

如图 4-44 所示的网络拓扑，某企业网络管理员发现网络中有异常流量，外网用户的恶意扫描探测，内网用户遭受病毒攻击后，会自动向外发送扫描，传播蠕虫等病毒，危害内网安全，希望通过 RG-IDS 端口扫描攻击的检测，初步识别攻击的源和目的，从而进行及时防御，将威胁降到最低，实现网络的安全防范功能。

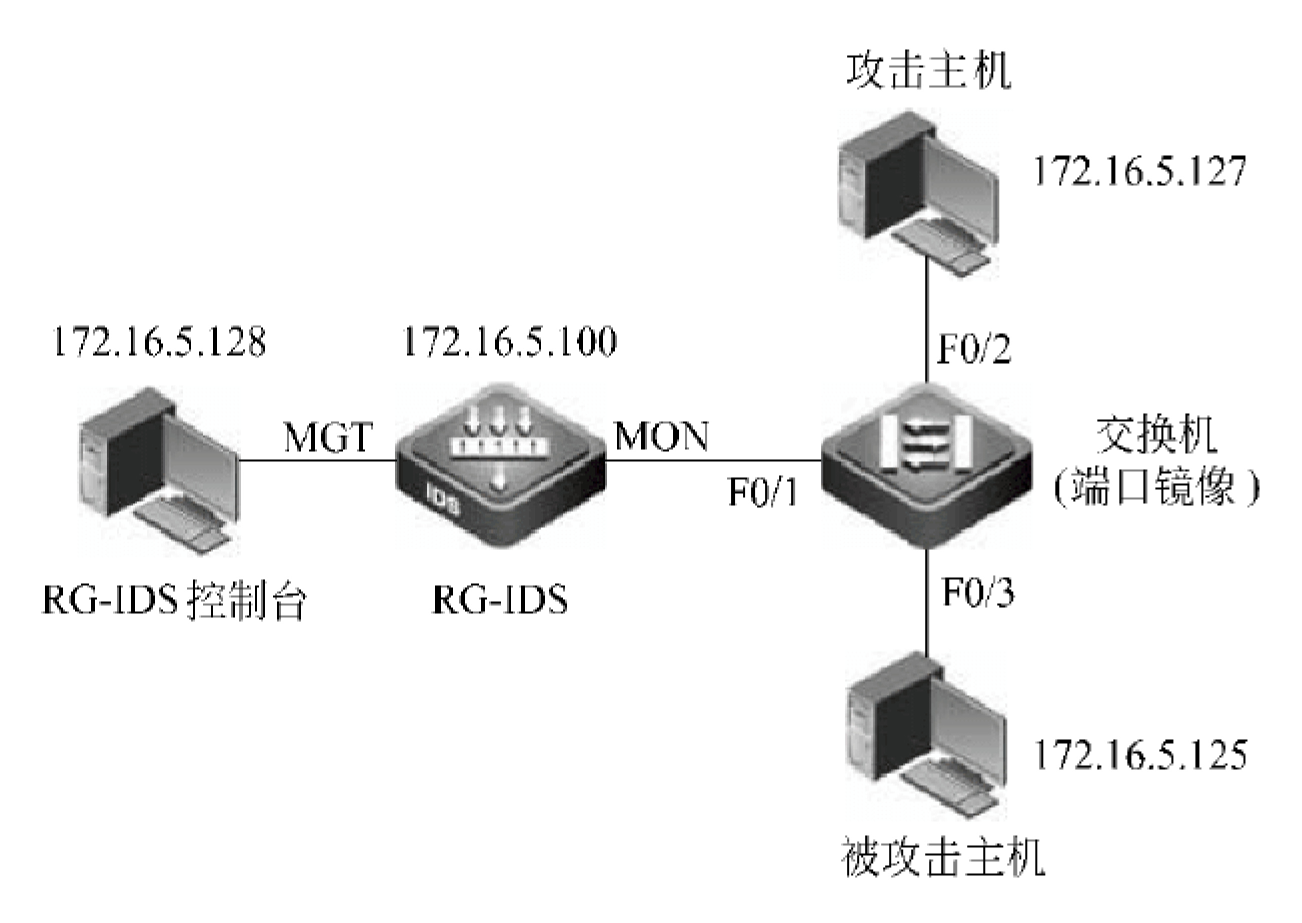



图 4-44　RG-IDS 端口扫描攻击检测网络拓扑图

## 【实验设备】

| | |
|---|---|
| PC | 3 台 |
| RG-IDS | 1 台 |
| 直连线 | 4 条 |
| 交换机 | 1 台(支持多对一的端口镜像) |
| 攻击工具 | portscan12(端口扫描工具) |

## 【预备知识】

- 交换机端口镜像配置。
- RG-IDS 配置。
- portscan12 攻击工具使用。

## 【实验原理】

端口扫描向目标主机的 TCP/IP 服务端口发送探测数据包,并记录目标主机的响应。通过分析响应来判断服务端口是打开的还是关闭的,就可以得知端口提供的服务或信息。端口扫描也可以通过捕获本地主机或服务器的流入/流出 IP 数据包来监视本地主机的运行情况,它仅能对接收到的数据进行分析,帮助我们发现目标主机的某些内在的弱点,而不会提供进入一个系统的详细步骤。

端口扫描技术行为作为恶意攻击的前奏,严重威胁用户的网络,RG-IDS 通过扫描的行为特征准确地识别出恶意的扫描行为,并及时通知管理员。

本实验通过攻击者常用的 portscan12 端口扫描工具进行端口扫描攻击,检验 RG-IDS 对端口扫描攻击的检测能力。

## 【实验步骤】

### 1. 策略编辑

如图 4-45 所示,单击主界面上"策略"按钮,切换到策略编辑器界面,从现有策略模板中生成一个新策略。在新的策略中选择 tcp:portscan 签名,并将策略下发到引擎中。

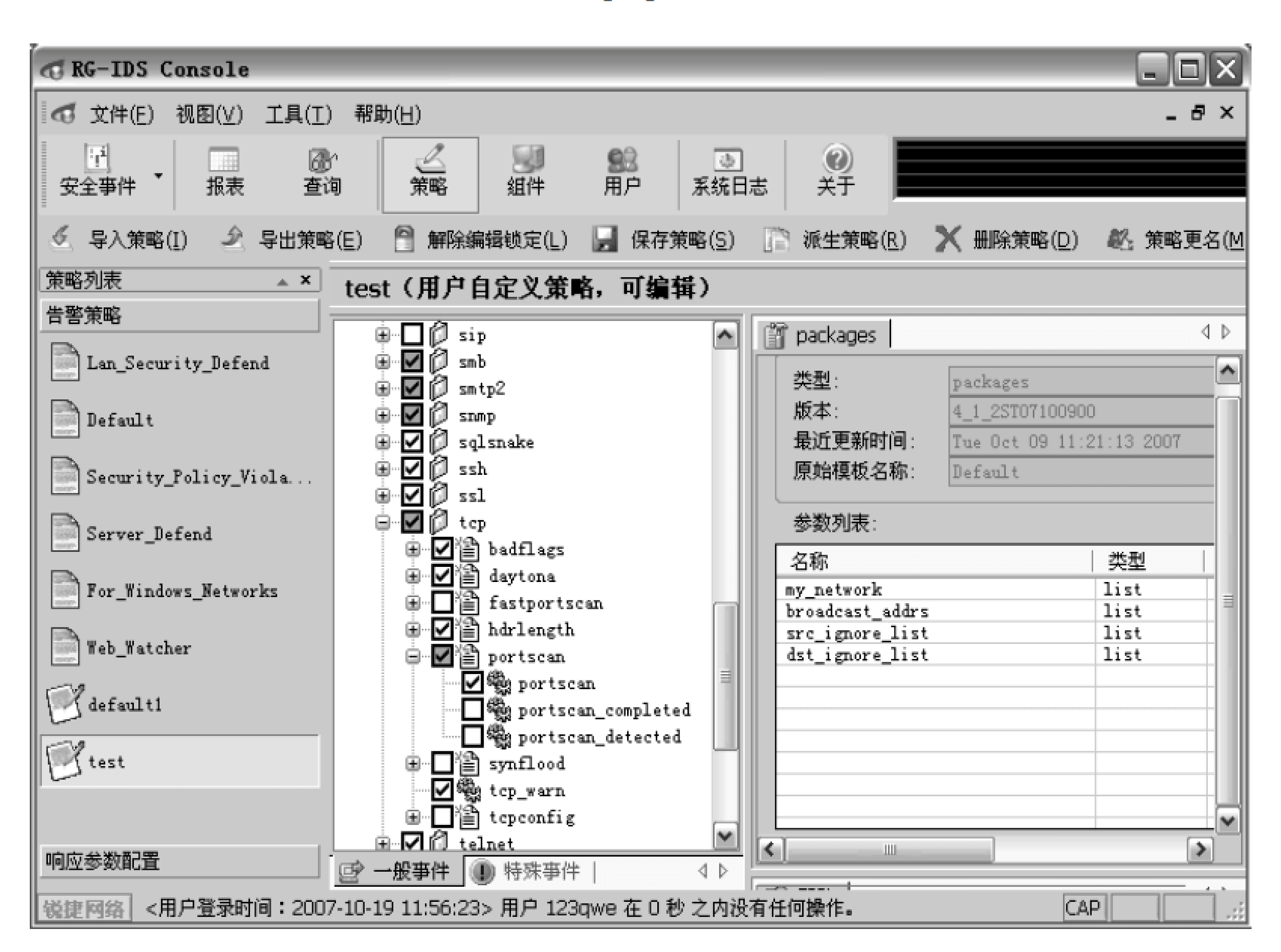



图 4-45　策略编辑器界面

## 2 实施攻击

双击 portscan12.exe PORTSCAN Custom ... 7th Sphere 文件，启动端口扫描攻击程序，如图 4-46 所示。

配置扫描参数，地址设置为 172.16.5.125，其他项不需要修改，如图 4-47 所示。

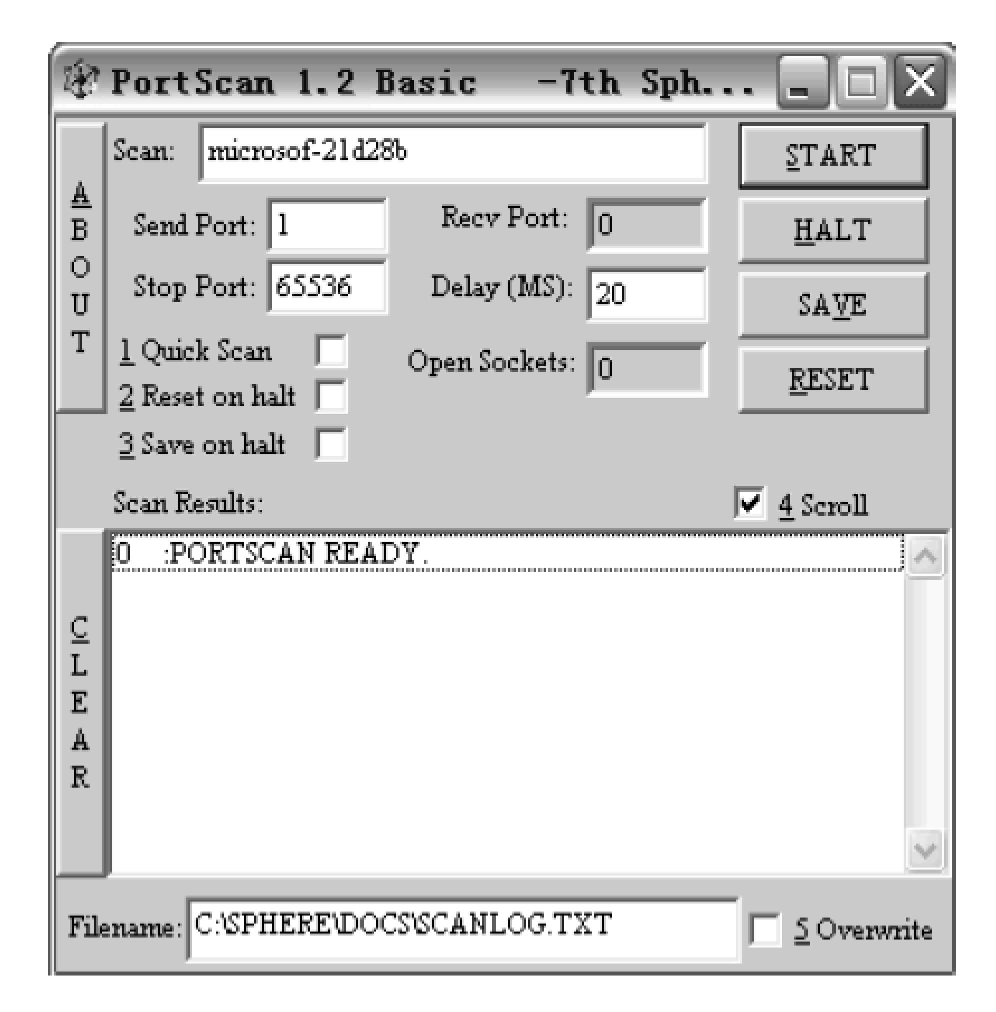



图 4-46 启动端口扫描攻击程序

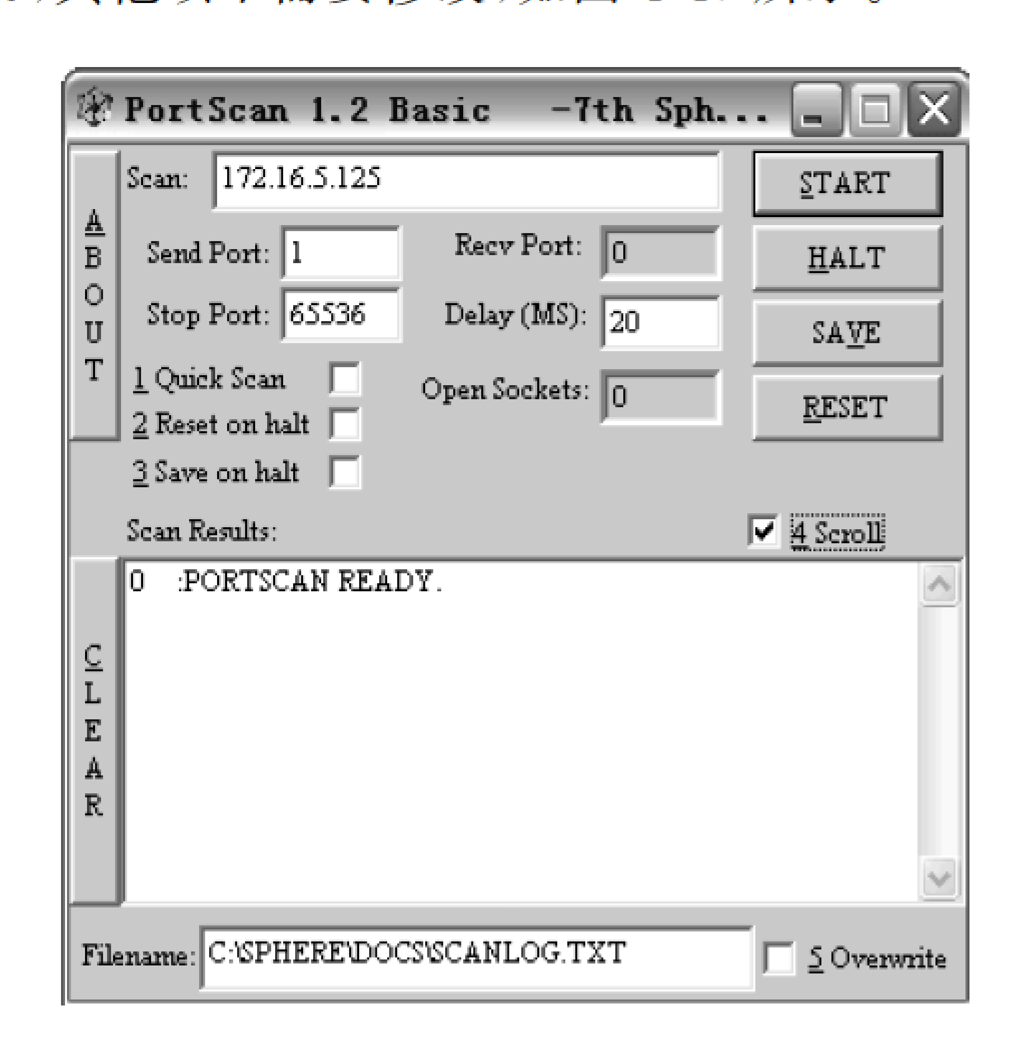



图 4-47 配置扫描参数

单击 START 按钮，开始扫描，扫描状态如图 4-48 所示。

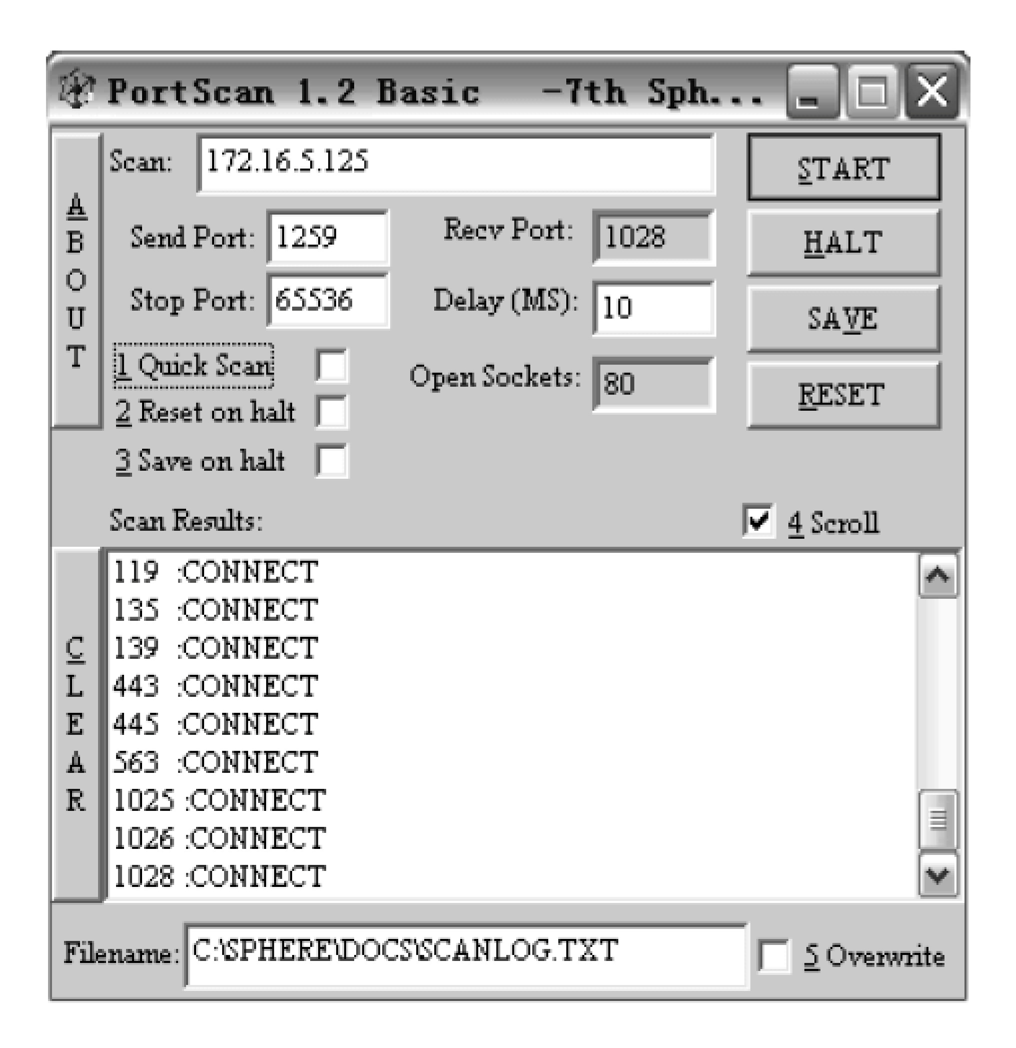



图 4-48 启动扫描功能

## 3. 查看安全事件信息

进入 RG-IDS 控制台，通过“安全事件”组件查看 IDS 检测的安全事件信息，如图 4-49 所示。

RG-IDS 将准确检测出 tcp:portscan 事件，事件详细信息如图 4-50 所示。

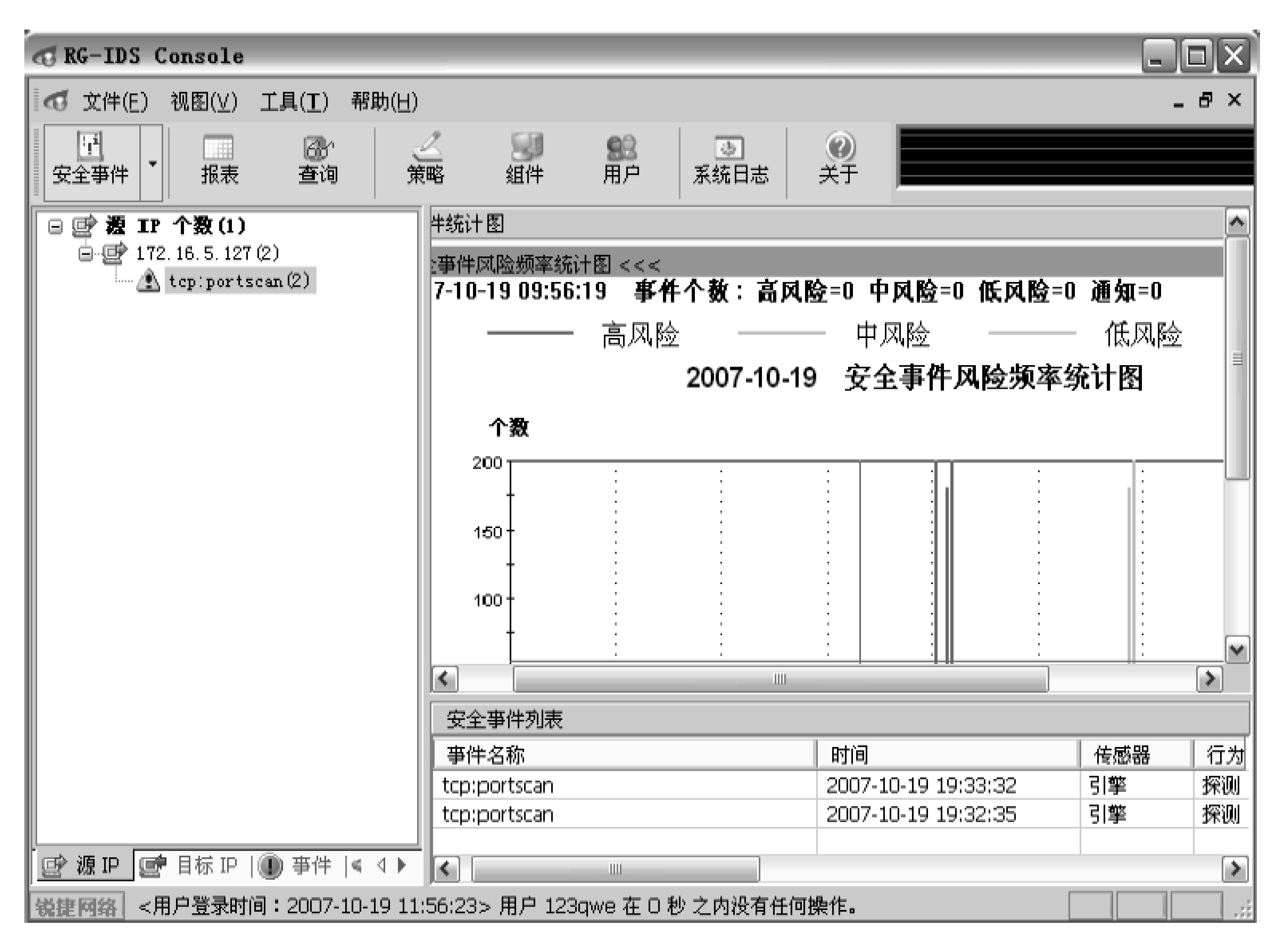



图 4-49　查看 IDS 检测的安全事件信息

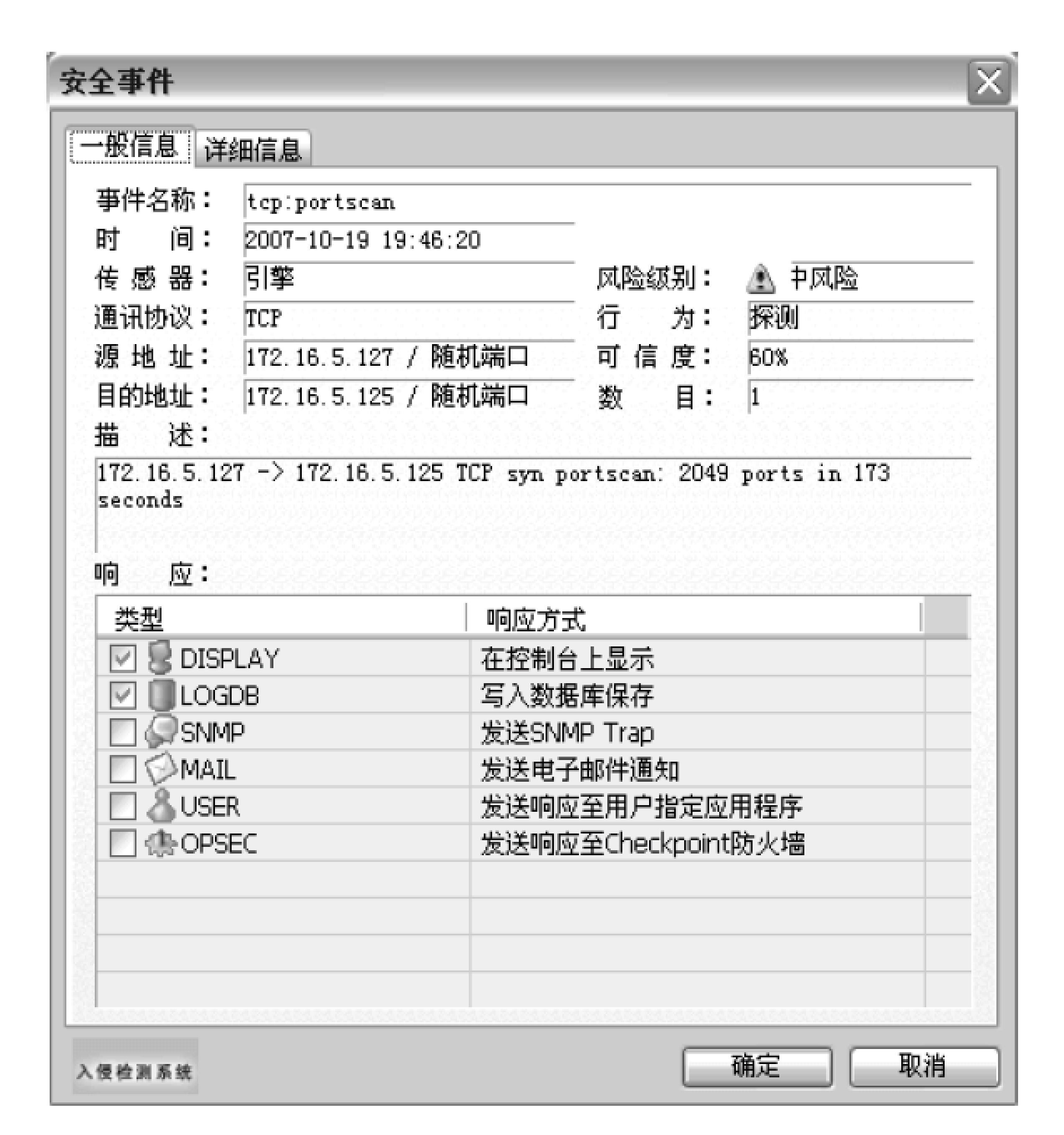



图 4-50　RG-IDS 检测出 tcp:portscan 事件

## 【注意事项】

- 攻击工具 portscan12.exe 只能用于实验使用,不可用于其他途径。
- 在实验过程中可以调节延时的长短 Delay (MS) 20 。
- 在实验过程中,可以通过选择 Quick Scan ☑ 来提高扫描的速度。

# 4.6 DoS 攻击检测

## 【实验名称】

DoS 攻击检测。

## 【实验目的】

使用 RG-IDS 对 DoS(Web CC)攻击进行检测。

## 【背景描述】

某网络中的 Web 服务器经常被外网用户扫描、探测和攻击,于是网络工程师部署了 IDS 系统以对各种攻击进行检测,以及对恶意扫描和探测行为进行审计。

## 【需求分析】

需求:CC 攻击采用 HTTP 方式,通过 GET 或 POST 方式在短时间里采用多线程方式访问 Web Server 中比较消耗计算机资源的一种攻击方式。在网络中对外发布的 Web Server 很容易受到此类攻击,而使服务器瘫痪,无法正常工作和响应正常的 Web 访问请求。

分析:通过 IDS 对 Web CC 攻击进行检测,初步识别攻击的源和目的,从而进行及时防御,将威胁降到最低,更好地提高网络安全性。

## 【实验拓扑】

如图 4-51 所示的网络拓扑,某企业网络管理员发现网络中的 Web 服务器经常被外网用户扫描、探测和攻击,于是部署了 IDS 系统对各种攻击进行检测,以及对恶意扫描和探测行为进行审计,以实现网络的安全防范功能。

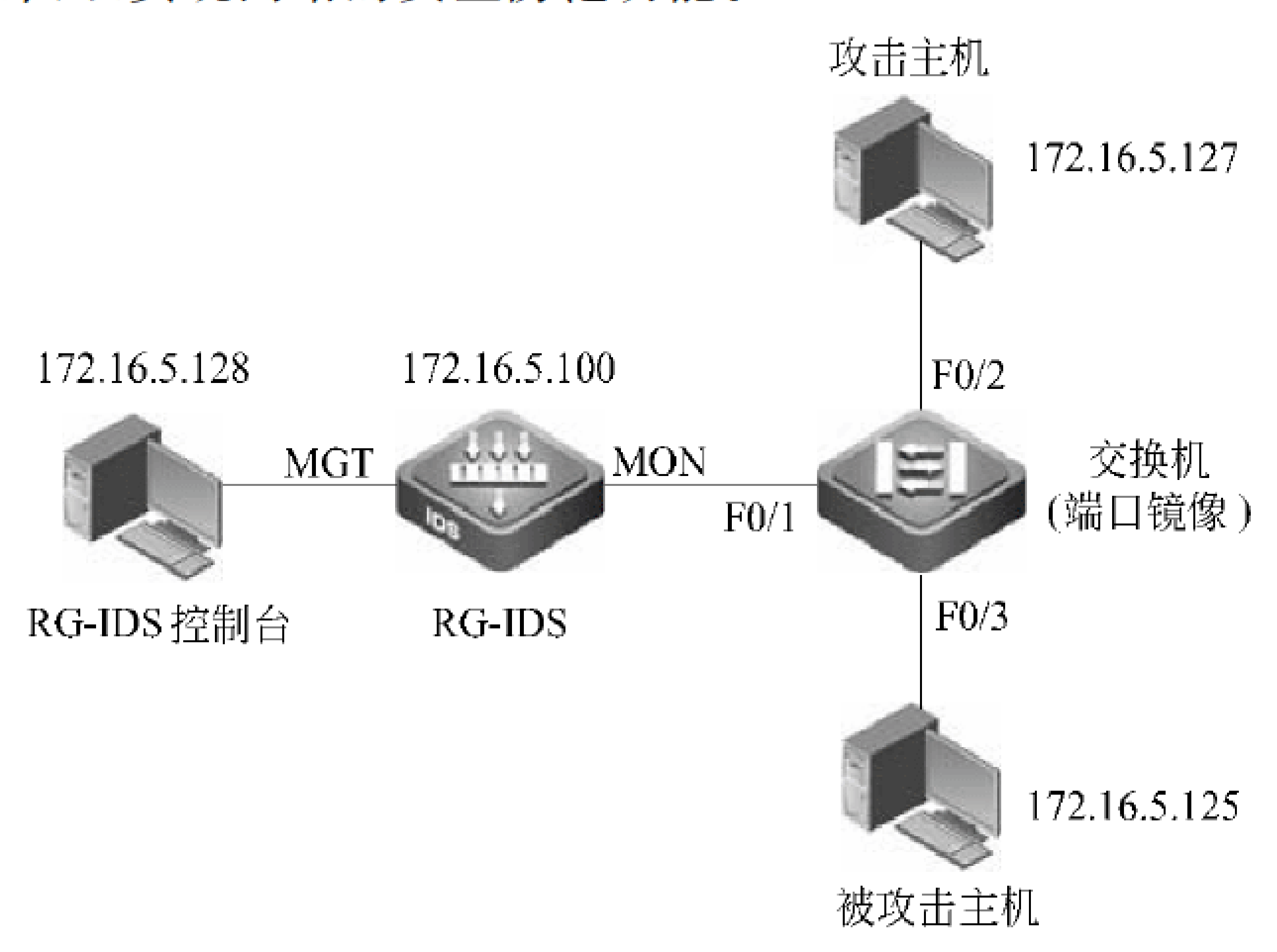



图 4-51　RG-IDS 对 DoS 攻击检测网络拓扑图

## 【实验设备】

PC　　　　3 台
RG-IDS　　1 台
直连线　　4 条
交换机　　1 台(支持多对一的端口镜像)
攻击工具　Webcc.exe(Web CC 攻击工具)
工具软件　Webserverv12.exe(Web 服务器)

## 【预备知识】

- 交换机端口镜像配置。
- RG-IDS 配置。
- Web CC 攻击工具。
- Webserverv12.exe 使用。

## 【实验原理】

Web DoS 主要用来攻击 Web 页面。攻击者向目标主机上比较大的 CGI 页面发起 HTTP 请求,造成目标主机拒绝服务。攻击者模拟多个用户(多少线程就是多少用户)不停地进行访问,访问那些需要大量数据操作,即需要消耗大量 CPU 资源的页面。这种攻击和正常的 Web 访问很类似,因此攻击者可以很好地隐藏自己,也可以绕开防火墙对目标主机进行攻击。

Web CC 攻击方法较为简单,易被黑客所掌握。因此,此类攻击严重威胁用户正常的 Web 资源,RG-IDS 通过行为特征准确地识别出恶意的行为,并及时产生告警。

## 【实验步骤】

### 1. 搭建 Web 服务器

将 Webserverv12.exe 工具复制到被攻击主机 172.16.5.125 中,并运行该软件,使被攻击主机不用做任何配置即可当做一台简易的 Web 服务器,如图 4-52 所示。




图 4-52　搭建 Web 服务器

该软件不需要做任何配置。如果被攻击主机本身已经被配置为 Web 服务器,则不需要运行此软件。

## 2 策略编辑

单击主界面上的“策略”按钮,切换到策略编辑器界面,从现有的策略模板中生成一个新的策略。在新的策略中选择 www2 下的 Webcc 签名,设置该签名的参数:WebHOST 为 172.16.5.125,保存策略,并将策略应用到引擎设备上,如图 4-53 所示。

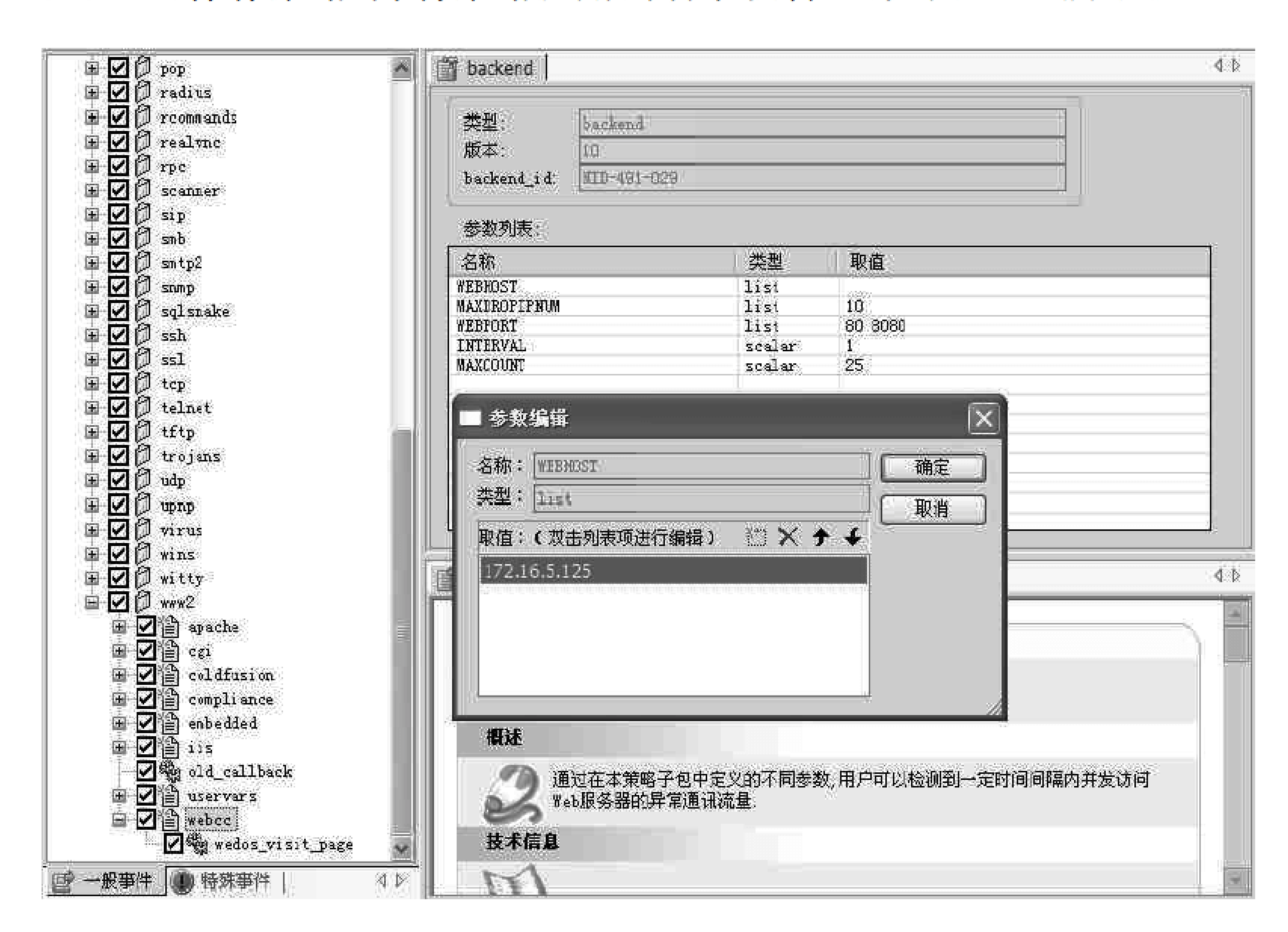


图 4-53　进行 RG-IDS 策略编辑

## 3 实施攻击

在 MS DoS 下运行 Webcc.exe 文件,启动 Web CC 攻击程序。命令格式为“Webcc 要攻击的 Web 服务器地址 要刷新的 Web 页的路径 要攻击的 Web 服务器端口”。例如,本实验环境可以使用 Webcc.exe 172.16.5.125 /index.html,如图 4-54 所示。

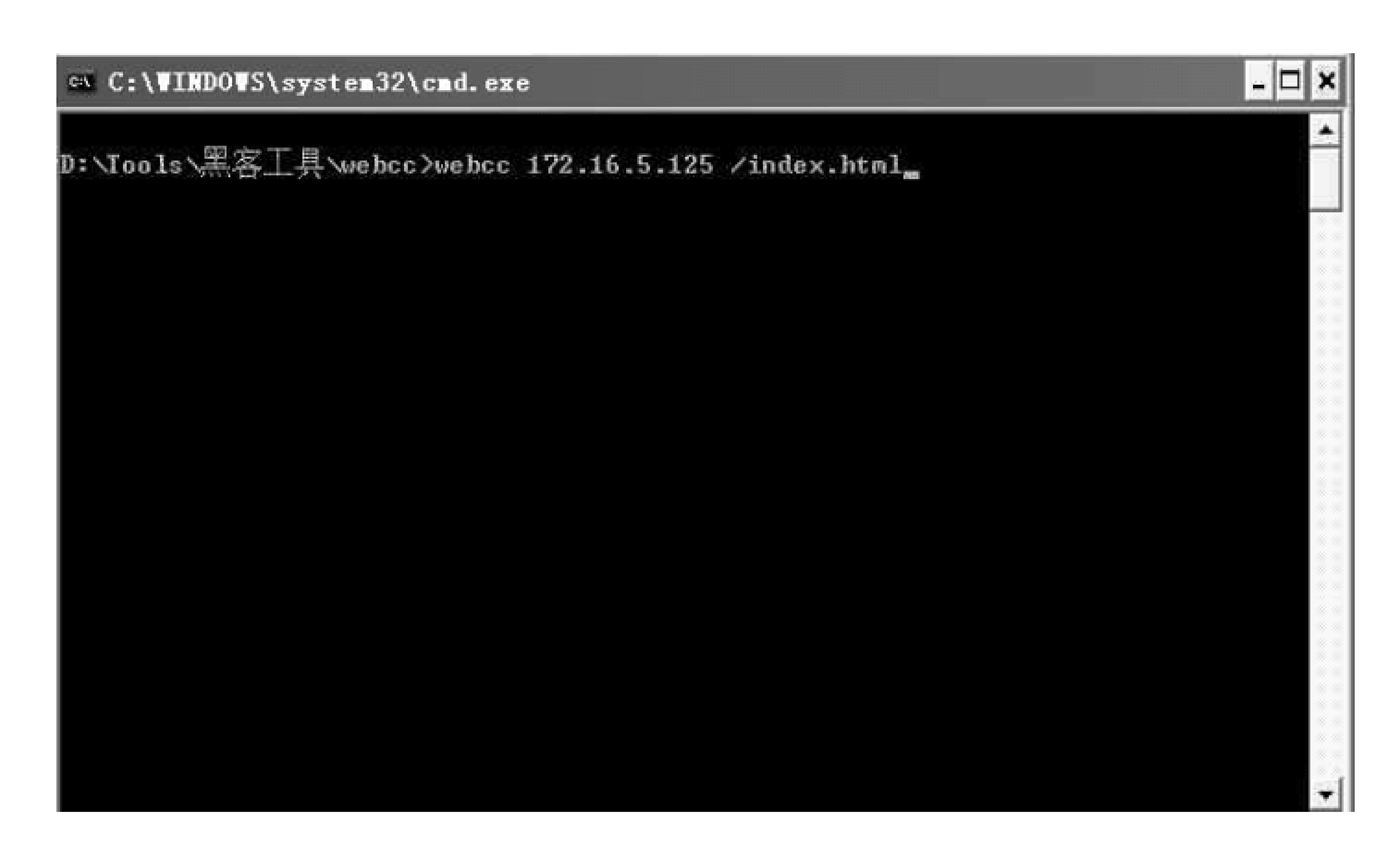



图 4-54　启动 Web CC 攻击程序

执行完毕后，在 IDS 控制台查看事件信息。

## 4. 查看警报

进入 RG-IDS 控制台，通过“安全事件”组件查看 IDS 检测的安全事件信息，如图 4-55 所示。

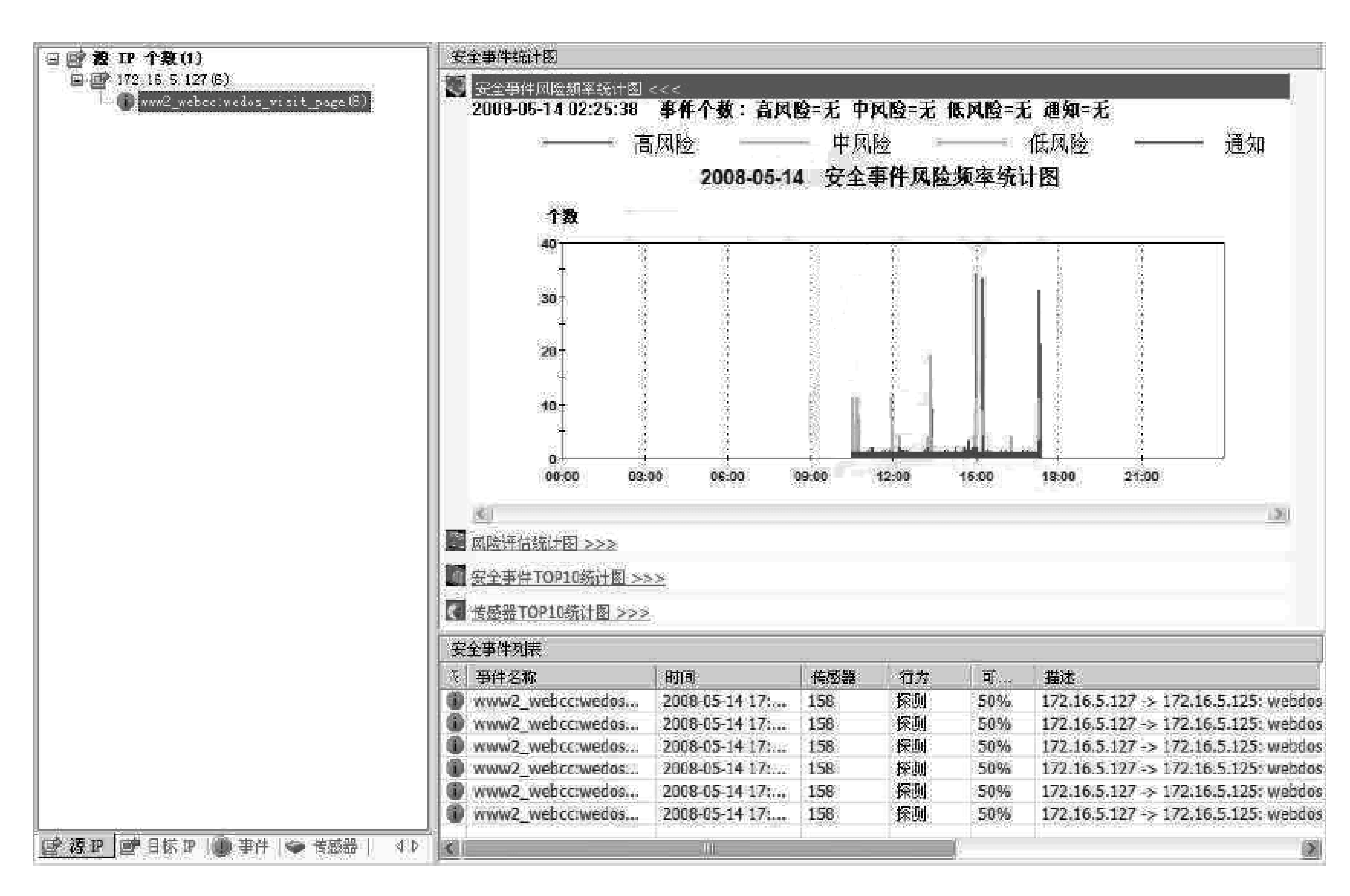



图 4-55 查看 IDS 检测的安全事件信息

RG-IDS 将准确检测出 Web CC 事件，事件详细信息如图 4-56 所示。

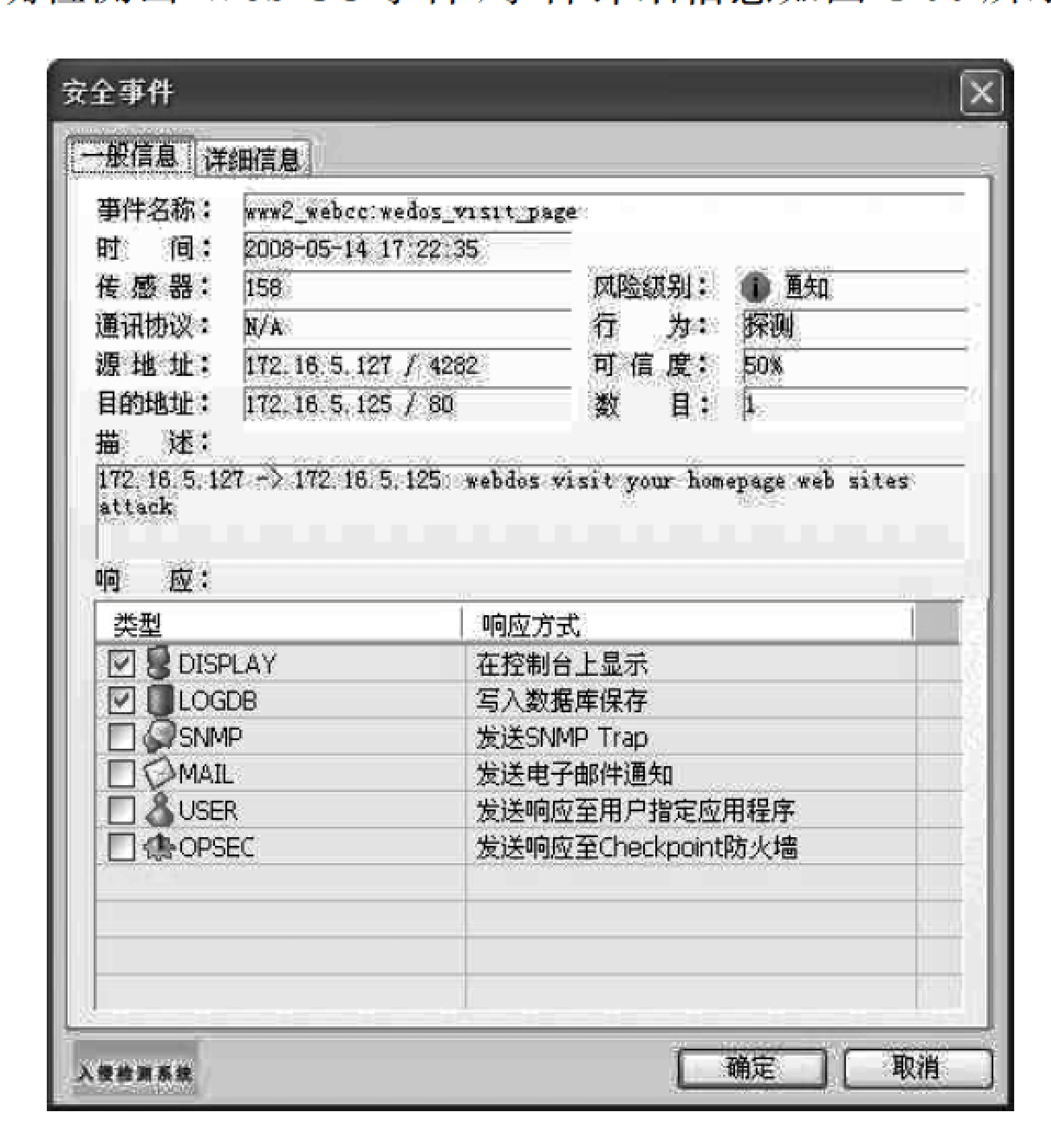



图 4-56 事件详细信息

【注意事项】

攻击工具 Webcc.exe 只能用于实验，不可用做其他途径。

www2：Webcc 主要参数功能说明如下：

- WebHOST

要保护的 Web 服务器地址，必须填才能生效。

该参数只支持 IPv4 格式，暂不支持域名格式。

- MAXDROPIPNUM

引擎最大缓存攻击 IP 数。

- WebPORT

HTTP 流量使用的端口。

认为包含 HTTP 流量的 TCP 数据包的端口号列表。

- INTERVAL

每一次刷新网页的时间间隔。

加大该参数会加大性能消耗，建议管理员使用默认配置。

- MAXCOUNT

特定 IP 在 INTERVAL 时间间隔内访问网页的最多次数。

该参数只针对客户端。

## 4.7 DDoS 攻击检测

【实验名称】

DDoS 攻击检测。

【实验目的】

使用 RG-IDS 对 DDoS 攻击进行检测。

【背景描述】

某网络中由于使用者的安全意识不强，经常遭受黑客的 DDoS 攻击，于是网络工程师部署了 IDS 系统对 DDoS 攻击进行检测。

【需求分析】

RG-IDS 能及时检测出 DDoS 攻击行为，并及时上报到控制台。

【实验拓扑】

如图 4-57 所示的网络拓扑，某企业网络管理员发现网络中使用者的安全意识不强，

经常遭受黑客的 DDoS 攻击，于是部署了 IDS 系统对 DDoS 攻击进行检测，以实现网络的安全防范功能。

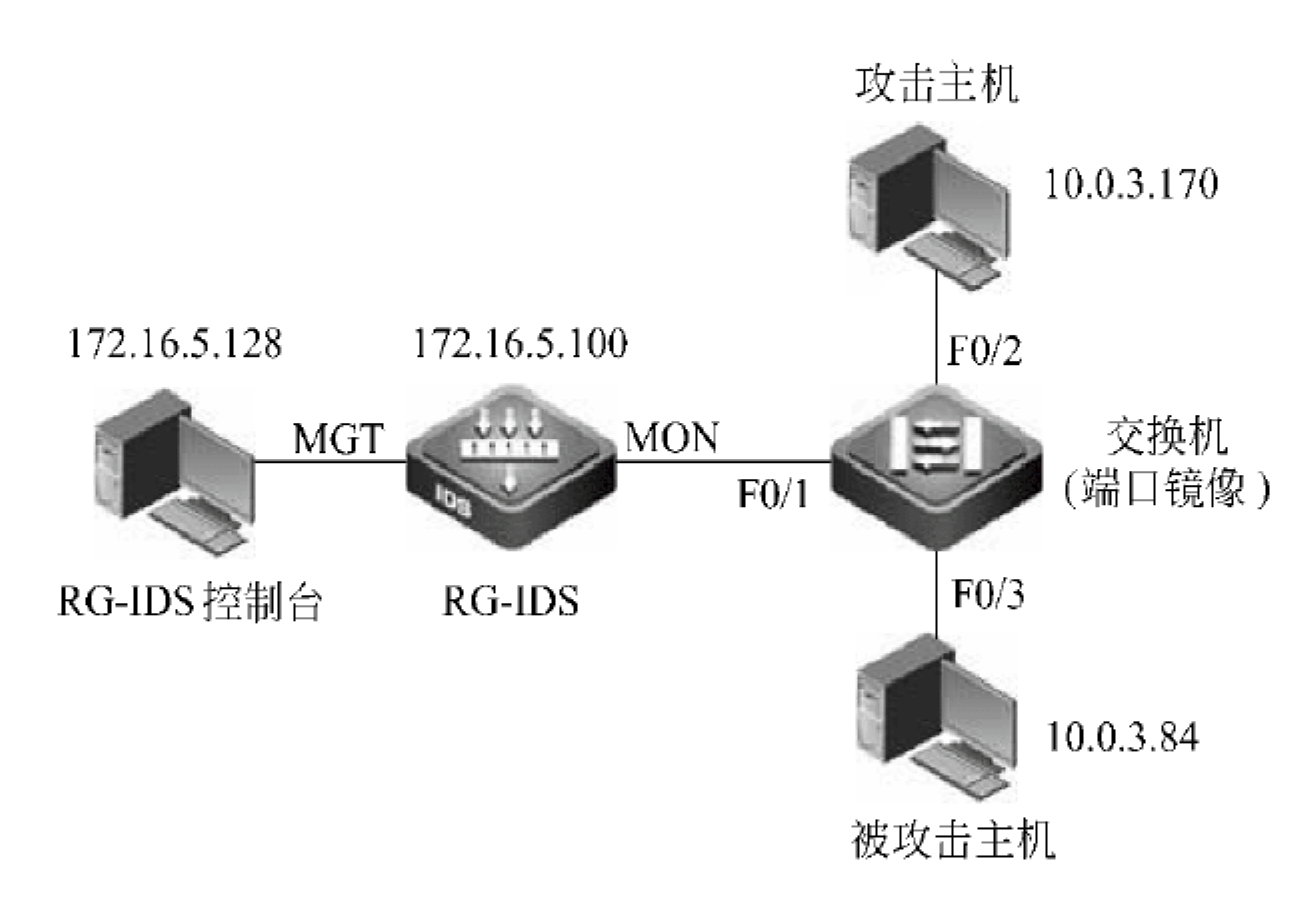



图 4-57　RG-IDS 对 DDoS 攻击检测网络拓扑图

## 【实验设备】

| | |
|---|---|
| PC | 3 台 |
| RG-IDS Sensor | 1 台 |
| 直连线 | 4 条 |
| 交换机 | 1 台(支持多对一的端口镜像) |
| 攻击工具 | DDoSPing |

## 【预备知识】

- 交换机端口镜像配置。
- RG-IDS 配置。

## 【实验原理】

DDoS(分布式拒绝服务攻击)广义上可以指任何导致用户的服务器不能正常提供服务的分布式攻击。造成拒绝服务攻击的原因很多，这里主要指通过网络进行的 DDoS 攻击。这种攻击使服务器充斥大量要求回复的信息，消耗网络带宽或系统资源，而导致网络或系统不胜负荷以至于瘫痪而停止提供正常的网络服务。

## 【实验步骤】

### 1. 策略编辑

如图 4-58 所示，单击主界面上的“策略”按钮，切换到策略编辑器左侧树状列表界面，从现有的策略模板中生成一个新的策略。在新的策略中选择 ddos：trinoo：trinoo_command 签名，并将策略下发到引擎中。

## 2 实施攻击

使用 DDoSPing 工具,在 Start IP address 以及 End IP address 文本框中分别填上被攻击主机的 IP 范围,然后单击右下角的 Configuration 按钮,如图 4-59 所示。

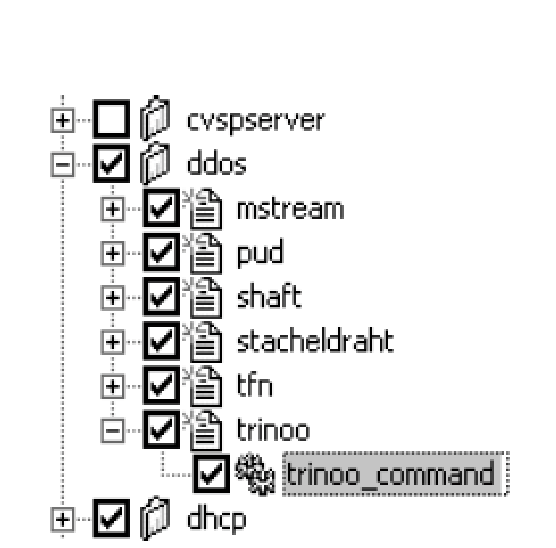



图 4-58 RG-IDS 策略编辑器界面

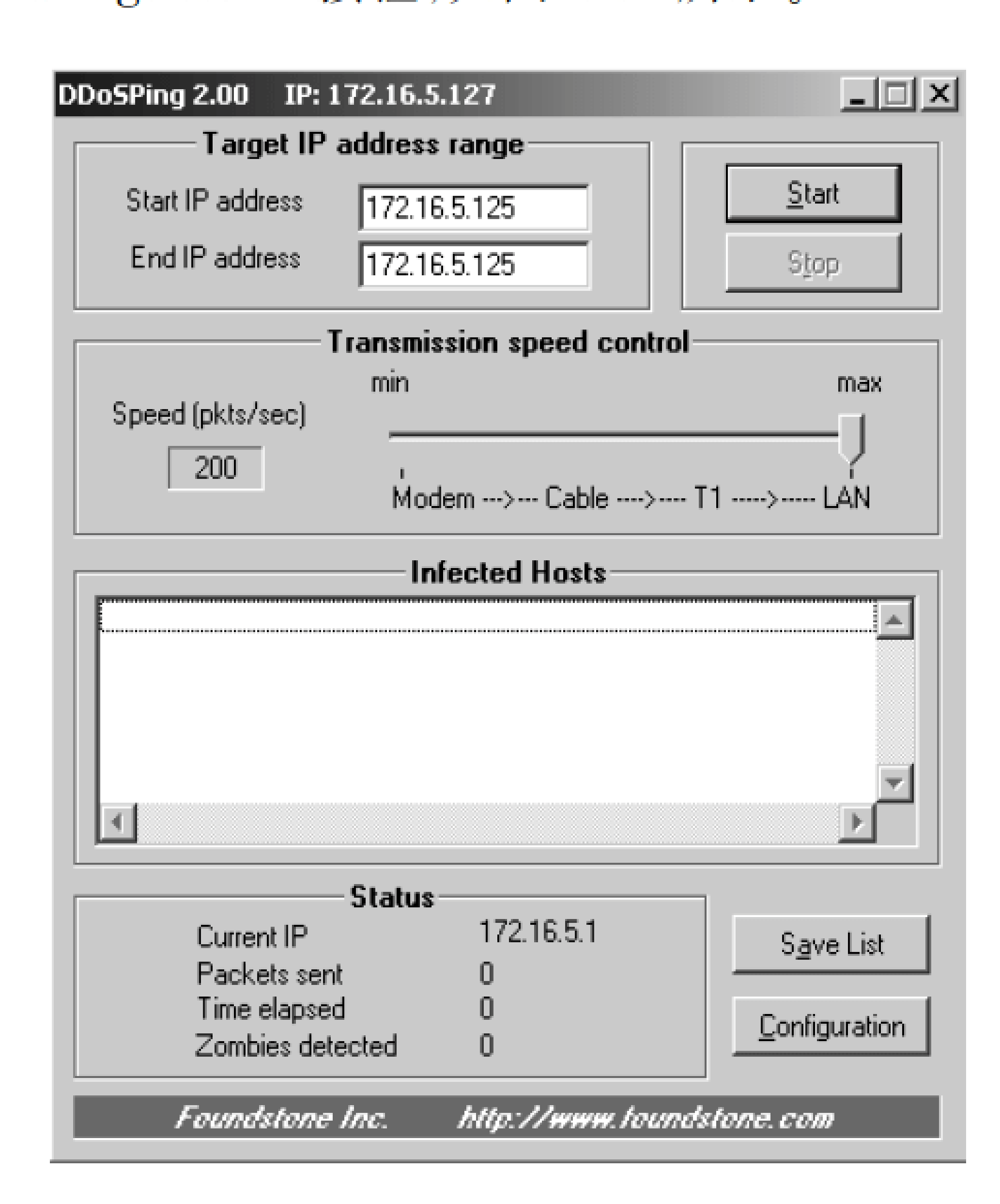



图 4-59 使用 DDoSPing 工具实施攻击(1)

具体配置如图 4-60 所示。

单击 OK 按钮,返回到程序主界面,单击右上角的 Start 按钮,如图 4-61 所示。

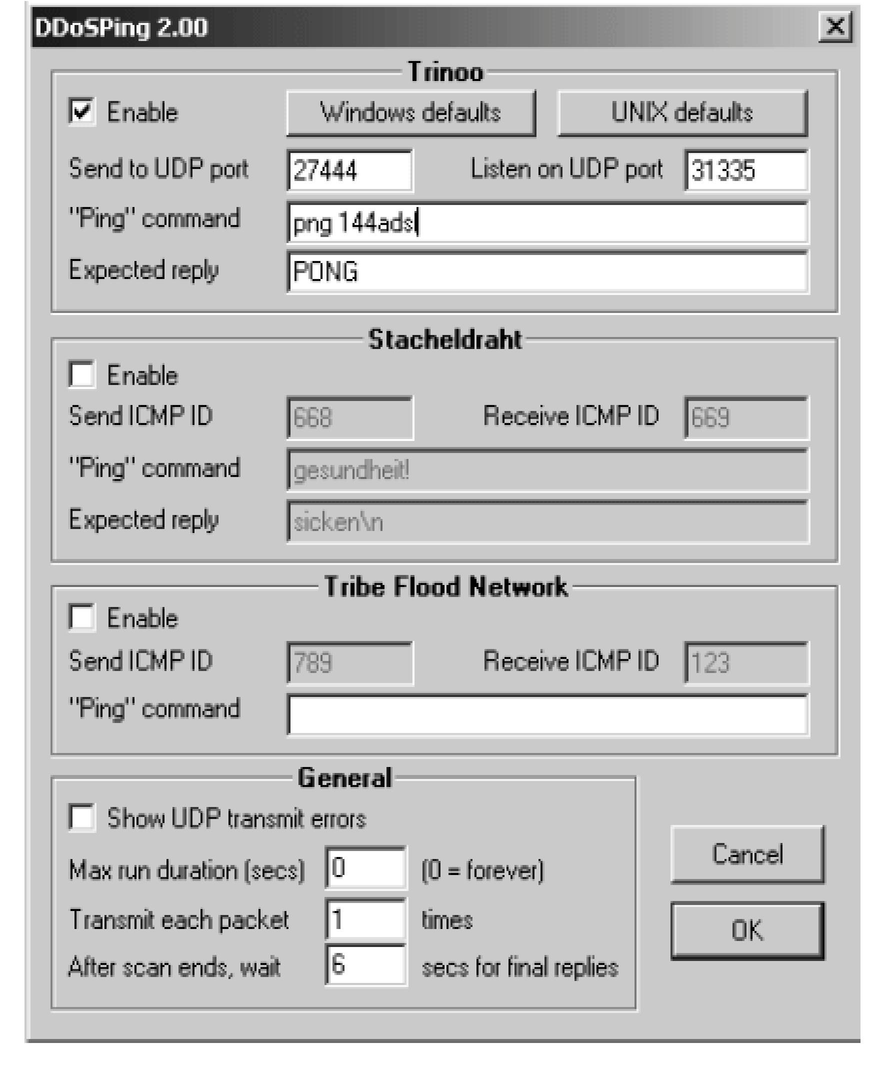



图 4-60 具体配置

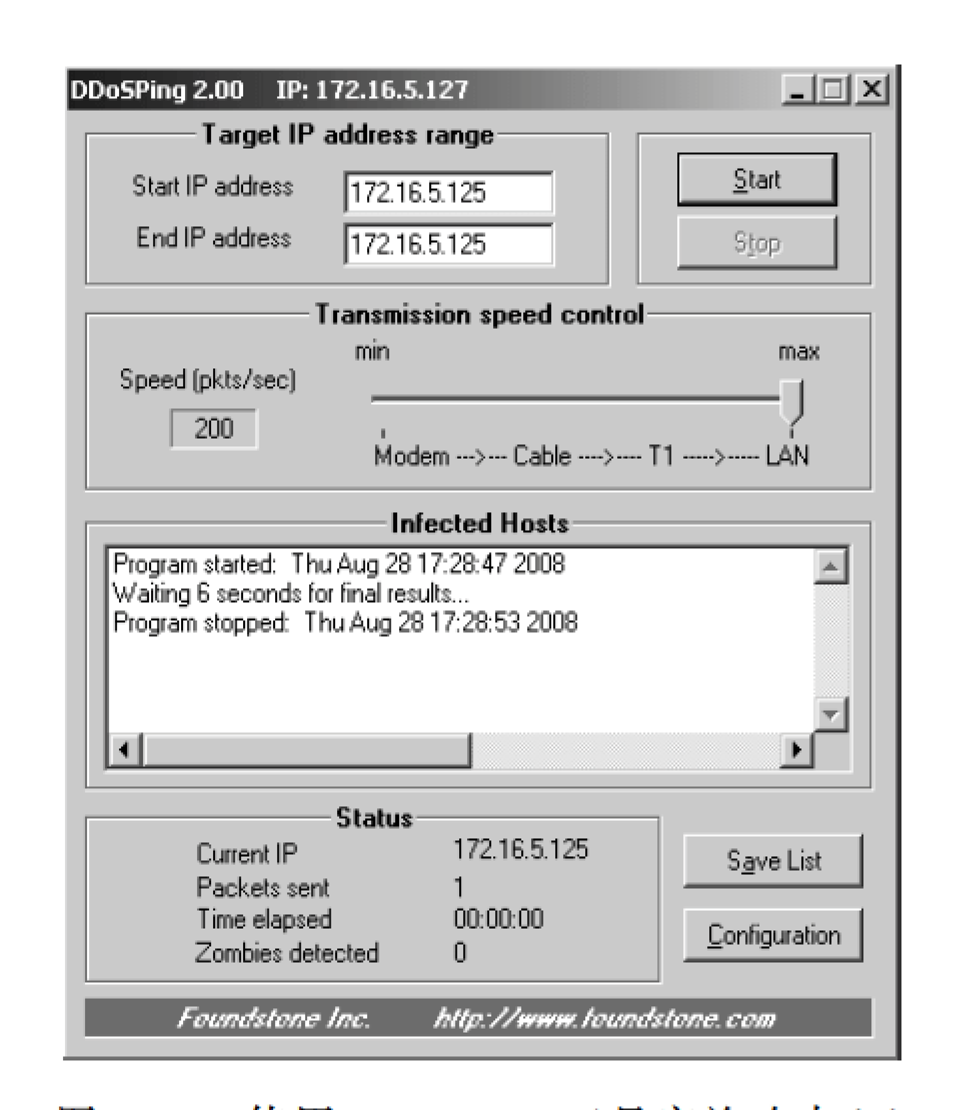



图 4-61 使用 DDoSPing 工具实施攻击(2)

## 3. 查看警报

进入 RG-IDS 控制台,通过“安全事件”组件查看 IDS 检测的安全事件信息,RG-IDS

将准确检测出 ddos_trinoo:trinoo_command 事件，如图 4-62 所示。

图 4-62　查看 IDS 检测的安全事件信息

事件详细信息如图 4-63 所示。




图 4-63　事件详细信息

## 【注意事项】

DDoSPing 工具只能用于实验。

# 4.8 密码策略审计

## 【实验名称】

密码策略审计。

## 【实验目的】

使用 RG-IDS 对网络服务的登录密码强度进行审计。

## 【背景描述】

某企业网络中使用 FTP 服务器提供文件传输服务。用户在访问 FTP 服务器之前需要进行身份验证。由于 FTP 服务器中存放了很多重要的数据和文件,所以需要用户使用高强度安全性的密码进行认证。

## 【需求分析】

需求:密码是最常见的一种认证形式,而且经常是外部和重要服务之间的唯一壁垒。攻击者可以使用一些程序来猜测或“破解”密码,但是通过选择一个安全的密码并做好必要的保密工作,就可以使未经授权却想非法进入服务变得非常困难。通常在组织内部对用户访问其重要服务器的密码安全均有强度等安全要求。

分析:通过 RG-IDS 实时检测和告警,使管理员及时发现使用不安全密码登录的用户,并及时进行必要的调整,降低不必要的风险。

## 【实验拓扑】

如图 4-64 所示的网络拓扑,某企业网络管理员发现在网络中使用 FTP 服务器,提供文件传输服务。用户在访问 FTP 服务器之前需要进行身份验证。由于 FTP 服务器中存

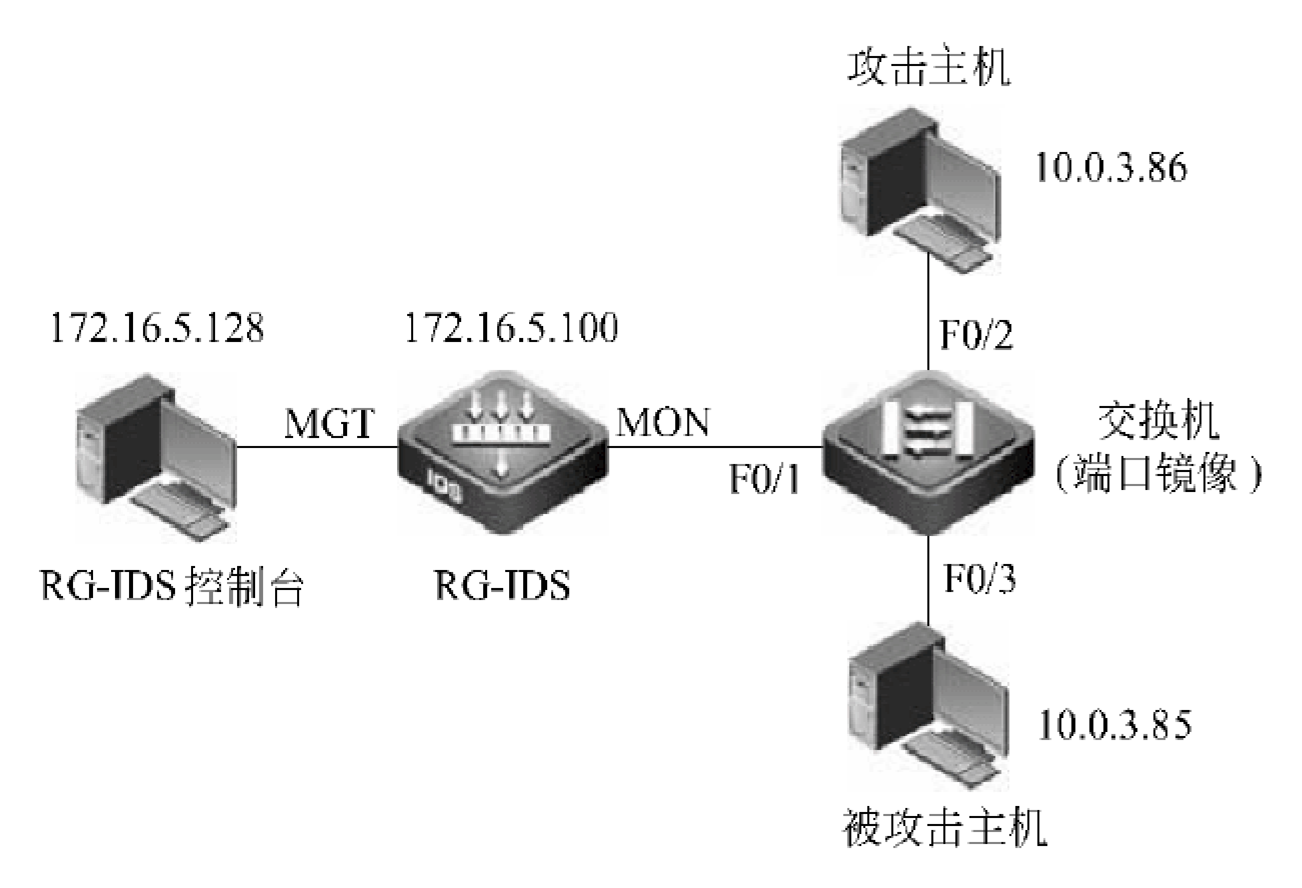



图 4-64　RG-IDS 密码策略审计网络拓扑图

放了很多重要数据和文件，所以需要用户使用高强度安全性密码进行认证，以实现网络安全防范功能。

## 【实验设备】

PC　　　　3 台
RG-IDS　　1 台
直连线　　4 条
交换机　　1 台(支持多对一的端口镜像)

## 【预备知识】

- 交换机端口镜像配置。
- RG-IDS 配置。
- FTP 服务器的配置。

## 【实验原理】

密码攻击是骇客攻击时最常用到的方式之一，利用密码的猜测、暴力破解等方法来掌握关键账号的密码，从而达到控制远程机器的目的。

防范此种攻击最常用的方法是保障密码的强度，即对账号所使用的密码长度、复杂度(使用大小写、字母、数字、非标准字符等进行组合)进行强制性控制。

本实验模拟某 FTP 服务器登录账号密码使用简单密码，IDS 将及时产生生告警。

## 【实验步骤】

### 1. 策略编辑

如图 4-65 所示，单击主界面上的“策略”按钮，切换到策略编辑器界面，从现有的策略模板中生成一个新的策略。在新的策略中选择 authentication：authentication 及 FTP，根据策略要求调整 authentication：authentication 的检测参数，将 PASSWORD_MATCH、NUMPASS 的值置为 1，并将策略下发到引擎中。




图 4-65　RG-ID 策略编辑器界面

### 2 使用弱密码进行登录

在 FTP 服务器上建立账户 test01 和 test02,密码分别是 123456 和 test02。在 FTP 客户端机器上分别使用账户 test01 和 test02 进行登录。

### 3. 查看警报

进入 RG-IDS 控制台,通过"安全事件"组件查看 IDS 检测的安全事件信息,如图 4-66 所示。

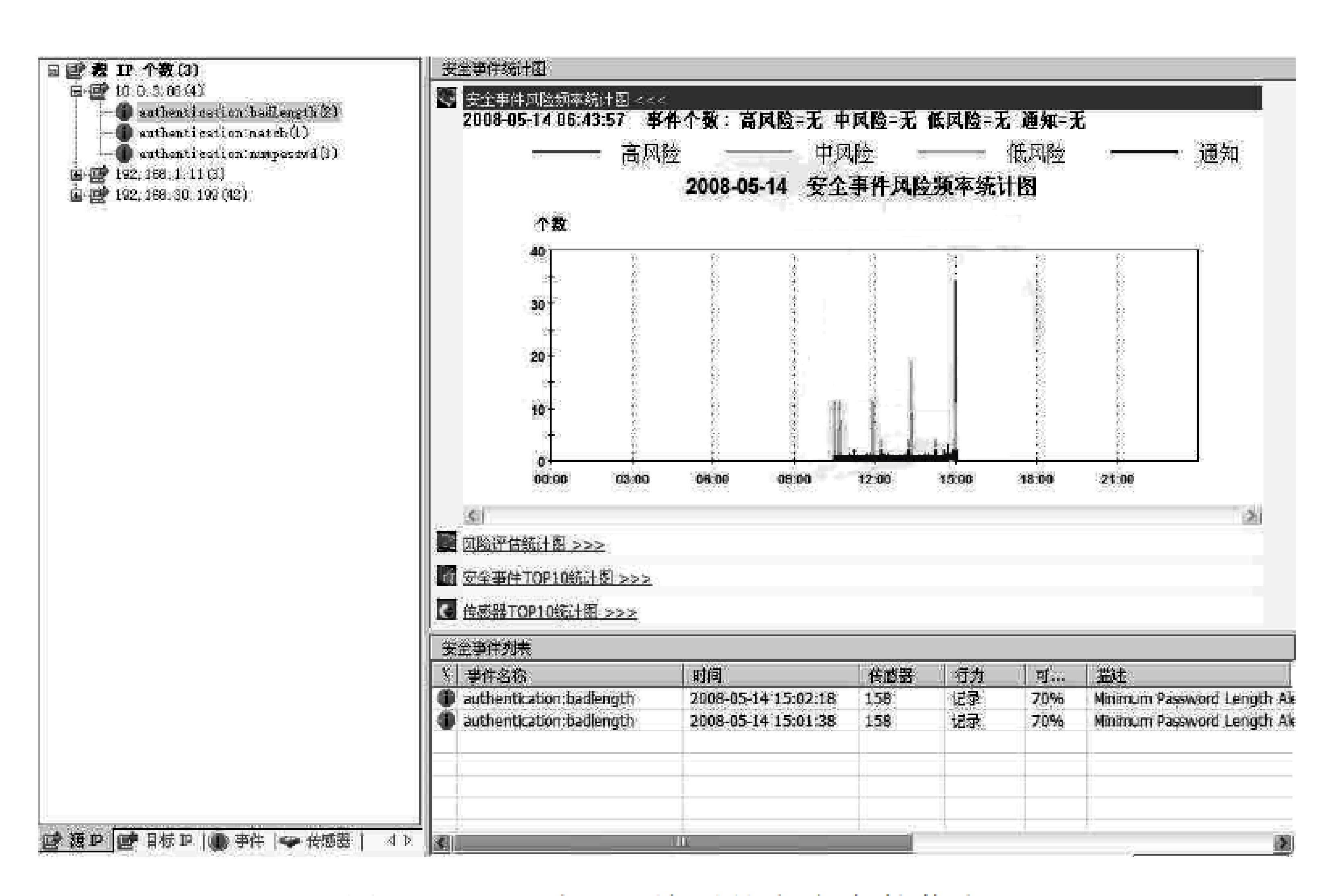



图 4-66　查看 IDS 检测的安全事件信息

RG-IDS 将准确检测出两次弱密码登录事件,事件详细信息如图 4-67 和图 4-68 所示。




图 4-67　RG-IDS 将准确检测出第一次弱密码登录事件




图 4-68　RG-IDS 将准确检测出第二次弱密码登录事件

## 4. 修改策略

在 RG-IDS 控制台中修改策略参数，将 ALERT PASSWORDS 值修改为 1，保存并应用策略到 IDS 当中，如图 4-69 所示。




图 4-69　在 RG-IDS 控制台中修改策略参数

## 5. 重新登录 FTP 服务器

重复第 2 步和第 3 步，观察安全事件详细信息的差异，在安全事件信息中将显示出不安全的密码，如图 4-70 和图 4-71 所示。

authentication：authentication 主要参数功能说明如下：

- ALERT_PASSWORDS

告警密码显示。

此值设置后用来判断是否需要在事件告警时显示用户口令信息。




图 4-70　RG-IDS 将准确检测出第一次弱密码登录事件




图 4-71　RG-IDS 将准确检测出第二次弱密码登录事件

- MIN_PASSWORD_LENGTH

触发事件告警的最短口令长度。

此策略值设置后，当告警的口令小于 8 位时，系统将进行告警。

- BAD_USER_LIST

错误的用户名列表。

触发事件告警的错误用户名称列表或不准确口令或用户名。

• BAD_PASSWORD_LIST

错误的口令列表。

触发事件告警的错误的或不安全的用户口令。

• BAD_SRC_IP

错误的源 IP 地址。

触发事件告警的源 IP 地址。

• BAD_DST_IP

错误的目的 IP 地址。

触发事件告警的目的 IP 地址。

• PASSWORD_MATCH

用户名和口令相同时是否触发事件告警。

此参数值设置为 1 时检测用户和口令匹配时触发告警，设置为 0 时不进行检测。

• NULLPASS

空口令。

参数值设置为 1 时当检测到口令为空时触发事件告警，设置为 0 时不告警。

• NUMPASS

数字口令。

参数值设置为 1 时当检测到口令仅为数字时触发事件告警，设置为 0 时不告警。

• ALPHAPASS

字母口令。

参数值设置为 1 时当检测到口令仅为字母时触发事件告警，设置为 0 时不告警。

• SPACEPASS

口令中有空格。

参数值设置为 1 时当检测到口令中有空格时触发事件告警，设置为 0 时不告警。

• WHITESPACEPASS

口令是空白(即没有输入任何键时)。

参数值设置为 1 时当检测到口令是空白时触发事件告警，设置为 0 时不告警。

• ALPHANUMPASS

字母和数字口令。

参数值设置为 1 时当检测到口令是字母和数字组成时触发事件告警，设置为 0 时不告警。

• ANONYMOUS_USERS

匿名用户列表。表中的匿名用户可以不受密码长度的限制。默认添加了部分知名的匿名用户。

# 4.9 IIS 服务漏洞攻击检测

## 【实验名称】

IIS 服务漏洞攻击检测。

## 【实验目的】

使用 RG-IDS 对 IIS 服务漏洞攻击进行检测。

## 【背景描述】

在某网络中使用 Windows 的 IIS 服务组件搭建了一个 Web 服务器。但是最近在网络中发现经常有针对 IIS 的攻击发生。于是网络工程师部署了 IDS 系统对各种攻击进行检测，以及对恶意扫描和探测行为进行审计。

## 【需求分析】

需求：IIS 4.0 和 IIS 5.0 在 Unicode 字符解码的实现中存在一个安全漏洞，导致用户可以远程通过 IIS 执行任意命令。当 IIS 打开文件时，如果该文件名包含 Unicode 字符，它会对其进行解码，如果用户提供一些特殊的编码，将导致 IIS 错误地打开或者执行某些 Web 根目录以外的文件。

分析：RG-IDS 能够实时地检测网络中针对 IIS 服务的攻击，并及时告警。

## 【实验拓扑】

如图 4-72 所示的网络拓扑，某企业网络管理员使用 Windows 的 IIS 服务组件搭建了一个 Web 服务器。但是最近在网络中发现经常有针对 IIS 的攻击发生。于是网络工程师部署了 IDS 系统以对各种攻击进行检测，以及对恶意扫描和探测行为进行审计，以实现网络的安全防范功能。

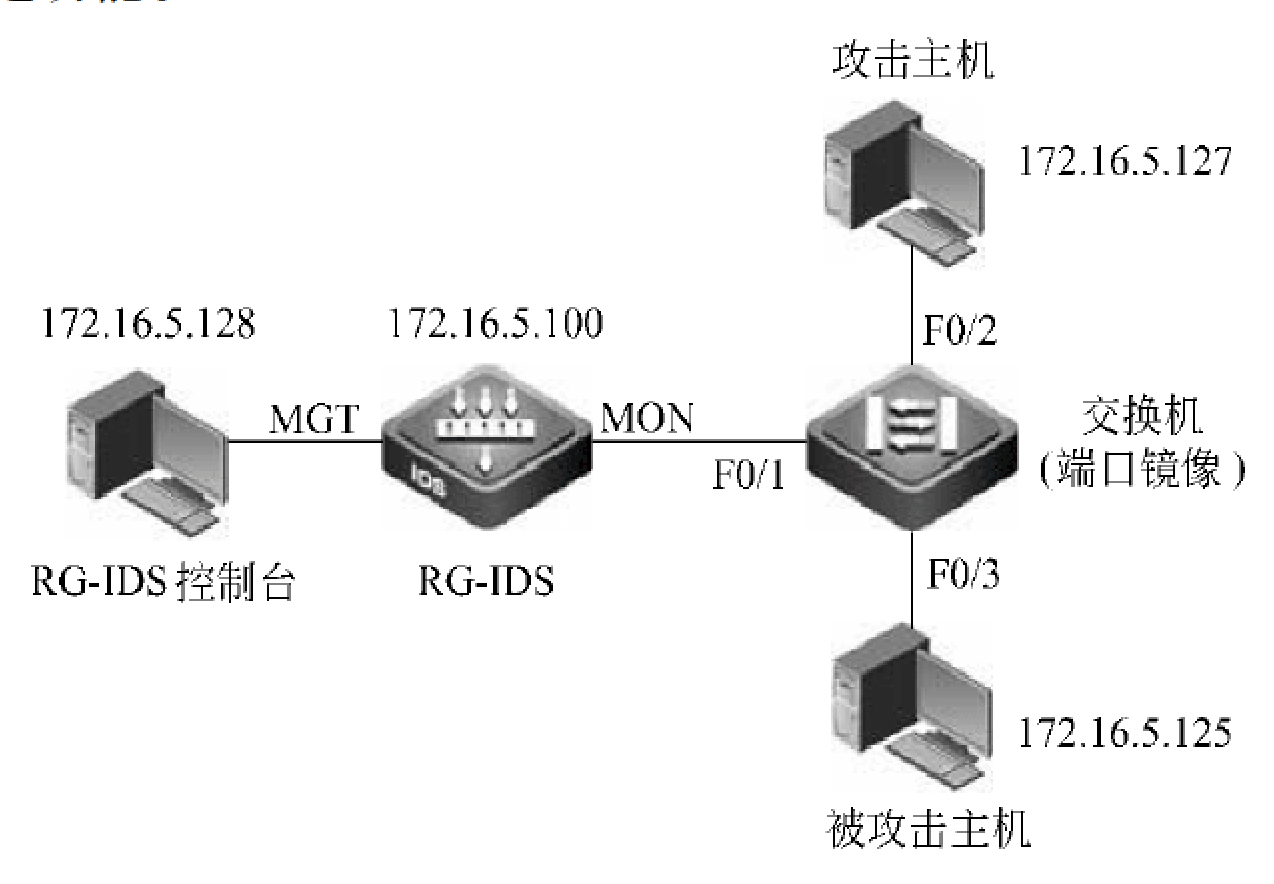



图 4-72　RG-IDS 对 IIS 服务漏洞攻击检测网络拓扑图

## 【实验设备】

| | |
|---|---|
| PC | 3 台 |
| RG-IDS | 1 台 |
| 直连线 | 4 条 |
| 交换机 | 1 台(支持多对一的端口镜像) |
| 攻击软件 | IIS Cracker.exe(IIS 攻击工具) |

## 【预备知识】

- 交换机端口镜像配置。
- RG-IDS 配置。
- IIS Cracker 操作。

## 【实验原理】

IIS(Internet Information Service)可以让有条件的用户轻易地建立一个本地化的网站服务器,同时提供 HTTP 访问、文件传输(FTP)服务以及邮件服务等。

但是 IIS 服务漏洞或缺口层出不穷,黑客不仅仅可以利用其漏洞停滞计算机的对外网络服务,更可修改其中的主页内容,甚至利用其漏洞进入到计算机内部,删改主机上的文件。以“扩展 UNICODE 目录遍历漏洞”为例,黑客就可以利用工具软件(如 IIS Cracker)进入到计算机内部。通过 IIS Cracker 入侵成功后,可以查看对方主机上的文件,通过远程控制入侵,黑客拥有对主机上的主页和文件进行窃取、修改和删除等权限。

本实验通过 IIS Cracker 工具攻击开放 IIS 服务的 Web 服务器并获得权限。RG-IDS 能及时准确地检测出该类攻击,并将警告上报给控制台。

## 【实验步骤】

### 1. 使用 Windows 的 IIS 组件搭建 Web 服务器

在 IIS 中搭建 Web 服务器的过程见相关资料,为不影响主题,此处略。

### 2. 策略编辑

如图 4-73 所示,单击主界面上的“策略”按钮,切换到策略编辑器界面,从现有的策略模板中生成一个新的策略。在新的策略中选择 www2:iis:nimda_scan_alert 签名,并将策略下发到引擎中。

### 3. 实施攻击

双击 IIS Cracker.exe IIS Cracker CNSFC Network Group 文件,启动 IIS 攻击程序,如图 4-74 所示。

配置攻击参数,将“当前连接”地址设置为 172.16.5.125,其他项不需要修改,如图 4-75 所示。



图 4-73　RG-ID 策略编辑器界面

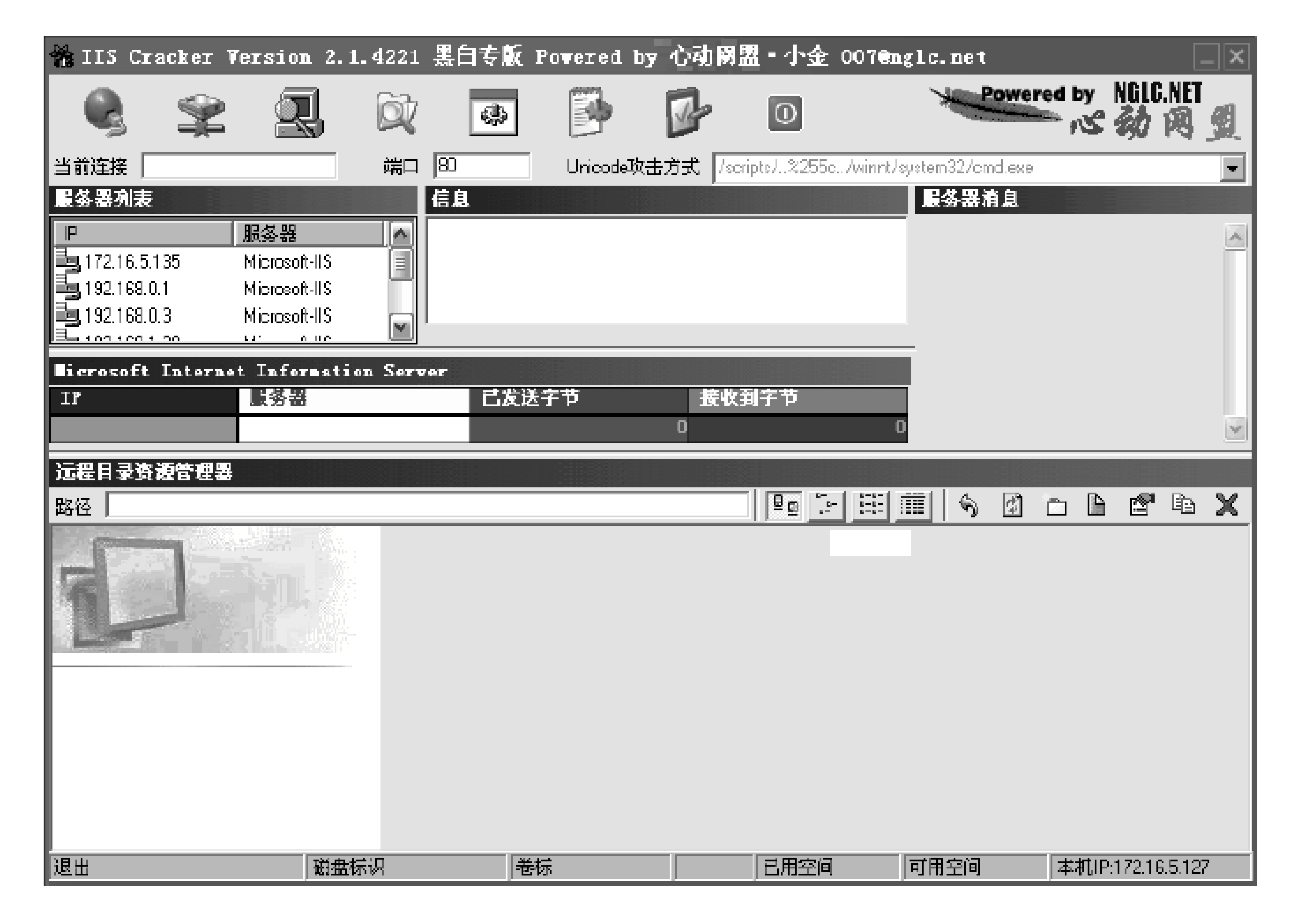


图 4-74　启动 IIS 攻击程序



图 4-75　配置攻击参数

单击 按钮，开始攻击。攻击完成后，可以在“远程目录资源管理器”区域中找到被攻击主机的文件目录，如图 4-76 所示。




图 4-76　找到被攻击主机的文件目录

单击 按钮，即可进入被攻击主机的系统目录，如图 4-77 所示。




图 4-77　进入被攻击主机的系统目录

### 4. 查看警报

进入 RG-IDS 控制台，通过“安全事件”组件查看 IDS 检测的安全事件信息，如图 4-78 所示。

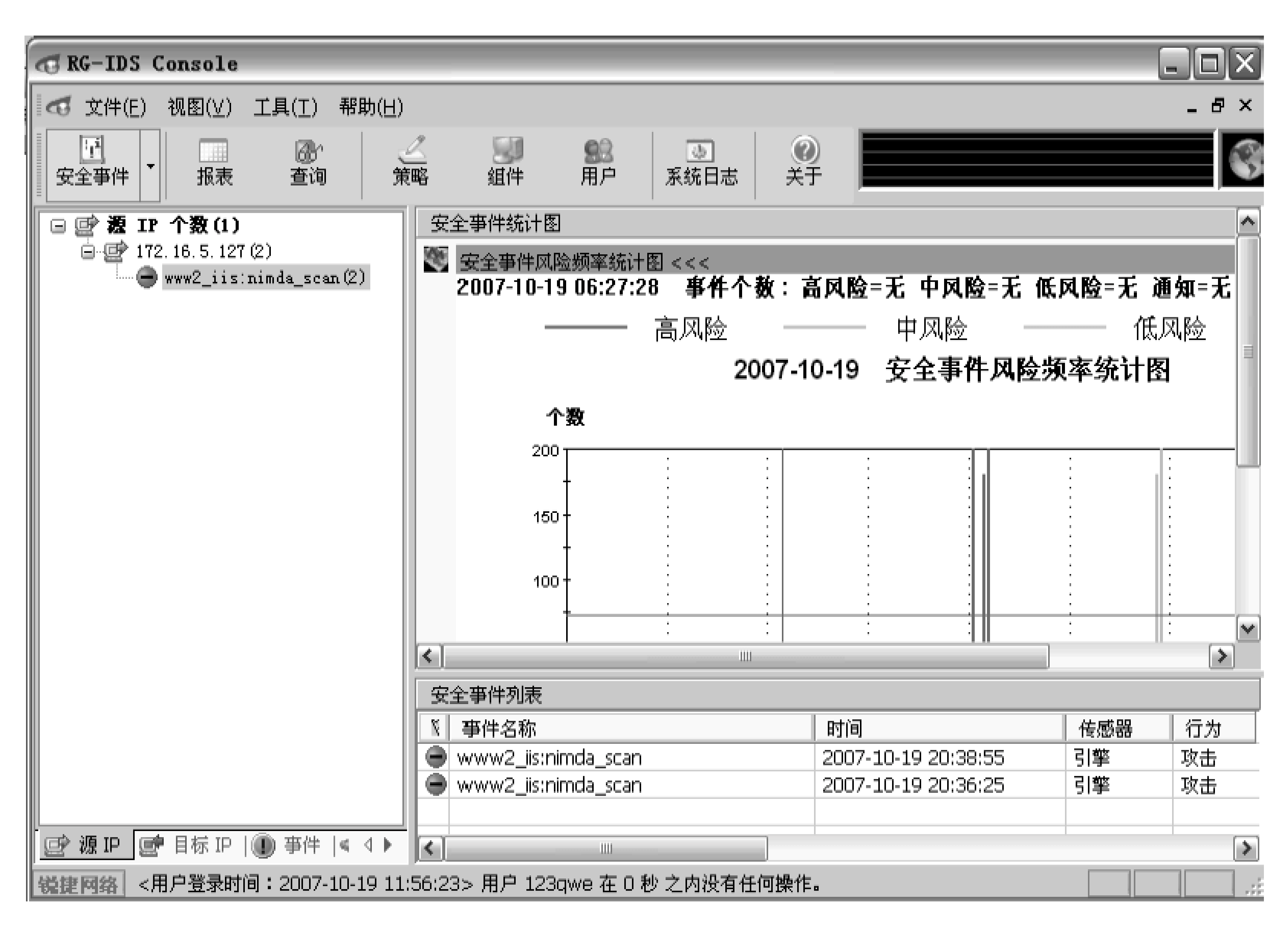


图 4-78 查看 IDS 检测的安全事件信息

RG-IDS 将准确检测出 www2:iis:nimda_scan_alert 事件，事件详细信息如图 4-79 所示。

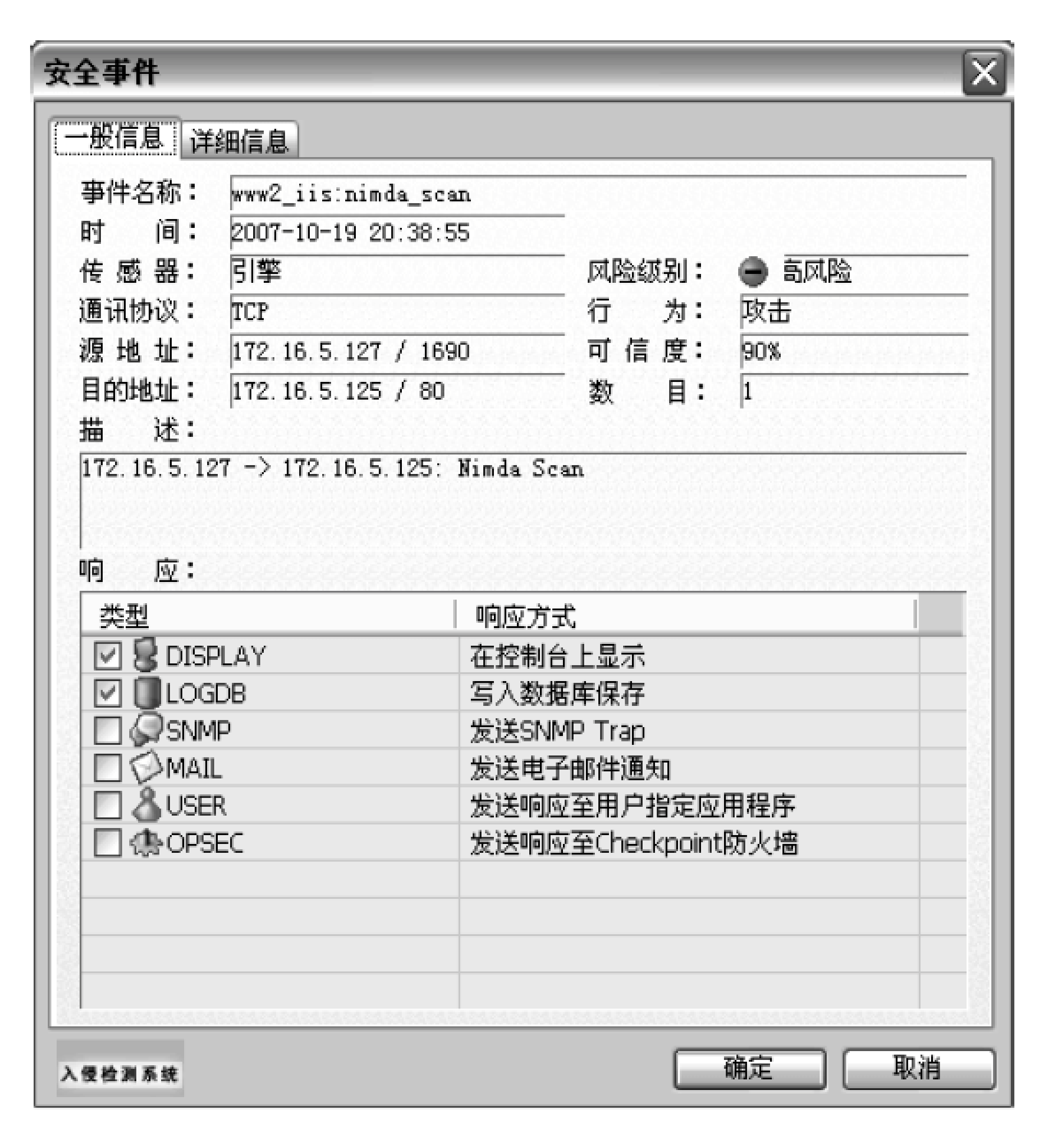


图 4-79 事件详细信息

【注意事项】

攻击工具 IIS Cracker 只能用于实验。

## 4.10　缓冲区溢出攻击检测

【实验名称】

缓冲区溢出攻击检测。

【实验目的】

使用 RG-IDS 对缓冲区溢出攻击进行检测。

【背景描述】

在某网络中很多主机使用 Windows 操作系统，但是发现在网络中经常有针对 Windows 系统的攻击发生。于是网络工程师部署了 IDS 系统对各种攻击进行检测，以及对恶意扫描和探测行为进行审计。

【需求分析】

为了检测针对 Windows 系统的攻击，可以部署 IDS 系统，并根据 IDS 产生的告警来定位攻击源。

【实验拓扑】

如图 4-80 所示的网络拓扑，某企业网络管理员发现很多主机使用 Windows 操作系统，经常有针对 Windows 系统的攻击发生。于是网络工程师部署了 IDS 系统对各种攻击进行检测，以及对恶意扫描和探测行为进行审计，以实现网络的安全防范功能。

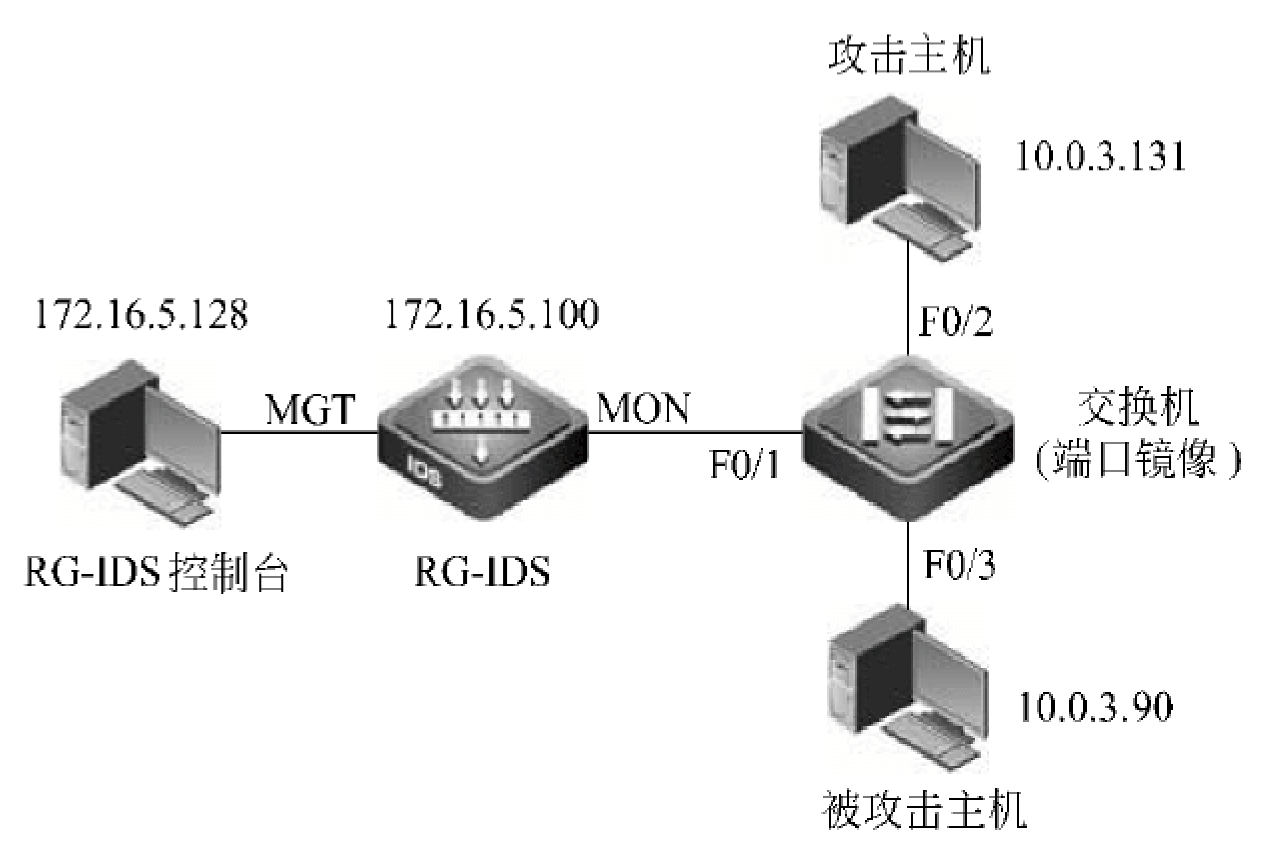



图 4-80　RG-IDS 对缓冲区溢出攻击进行检测网络拓扑图

## 【实验设备】

| | |
|---|---|
| PC | 3 台 |
| RG-IDS | 1 台 |
| 直连线 | 4 条 |
| 交换机 | 1 台(支持多对一的端口镜像) |
| 攻击软件 | metasploit V3.1 |
| 攻击主机 | Microsoft Windows 操作系统 |
| 被攻击主机 | Windows 2000 Server(未安装 Service Packet) |

## 【预备知识】

- 交换机端口镜像配置。
- RG-IDS 配置。
- metasploit 工具使用。

## 【实验原理】

Win32.Sasser.A 是一个通过 Windows 2000、Windows XP 和 Windows Server 2003 系统漏洞(MS04-011)传播的蠕虫病毒,病毒文件长度为 15872 字节。远程攻击者可以利用这个漏洞以 SYSTEM 权限在系统上执行任意指令,"震荡波"病毒就是利用这个漏洞产生的。

微软的 Server 服务中的漏洞可能允许远程执行代码,这是一个比较严重的漏洞,从 Windows 2000 SP4 到 Windows XP SP2 再到 Windows 2003 SP1,还有 64 位操作系统,无一幸免。这个漏洞的最著名的利用就是"魔波"(MS06-040)蠕虫病毒。

RG-IDS 检测该溢出攻击发生时的网络行为特征(基于客户系统已存在的漏洞)。

## 【实验步骤】

### 1. 策略编辑

如图 4-81 所示,单击主界面上的"策略"按钮,切换到策略编辑器界面,从现有的策略模板中生成一个新的策略。在新的策略中选择 msrpc:ms05039:upnp_ms05039 以及 msrpc:ms06040:srvsvc_ms06040_overflow 签名,并将策略下发到引擎中。

### 2 实施攻击

1) MS04-011

选择"开始"菜单中的-metasploit 3-metasploit 3 GUI 菜单项,启动 metasploit 攻击程序,如图 4-82 所示。

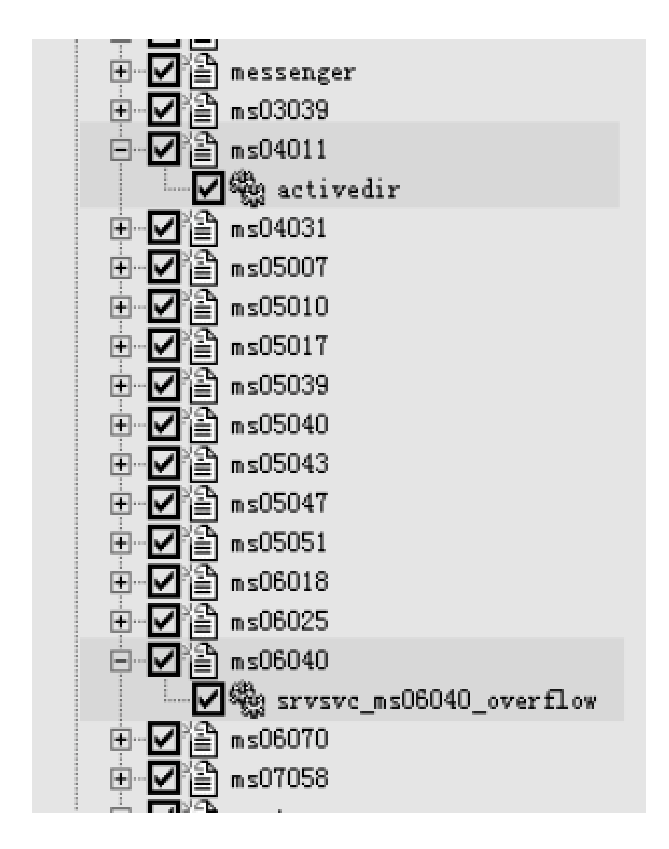



图 4-81　RG-ID 策略编辑器界面

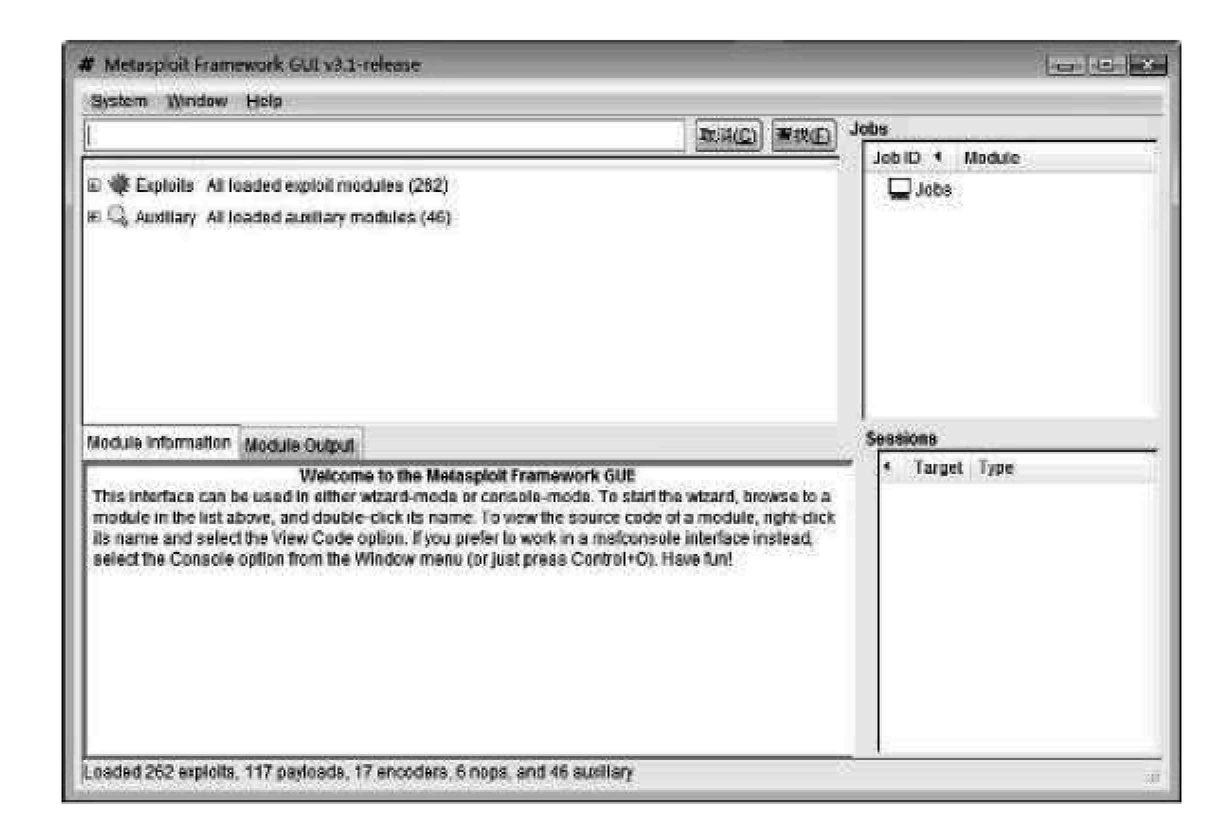



图 4-82　打开 metasploit 程序

依次选择 exploits-windows-smb，在下面的漏洞列表中双击 ms04_011_lsass，如图 4-83 所示。

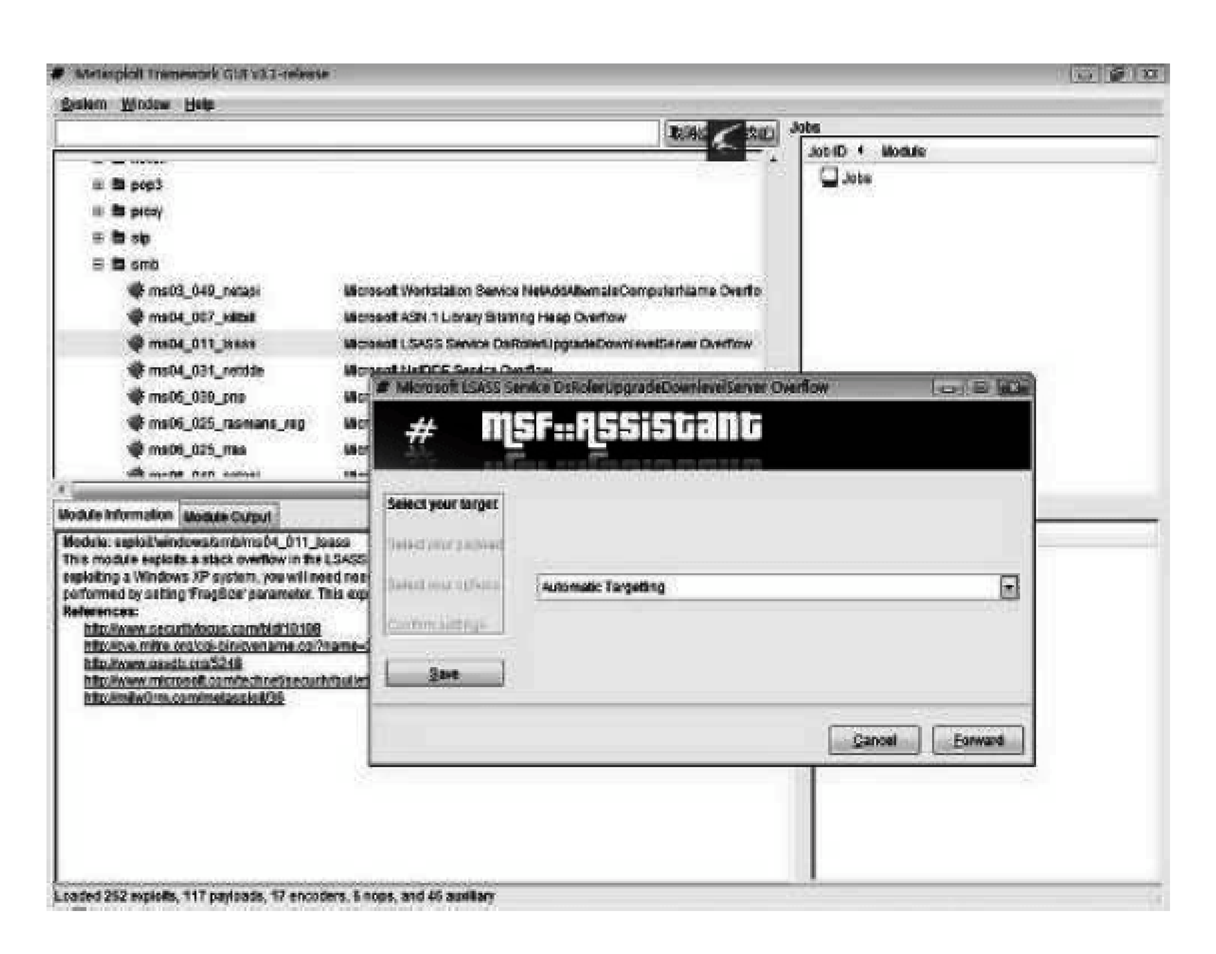



图 4-83　选择漏洞列表

按照下面的步骤在弹出的对话框中选择相应的参数，payload 选择 windows/shell_bind_tcp，RHOST 填上被攻击主机的 IP 地址，其他按默认选项，如图 4-84～图 4-87 所示。

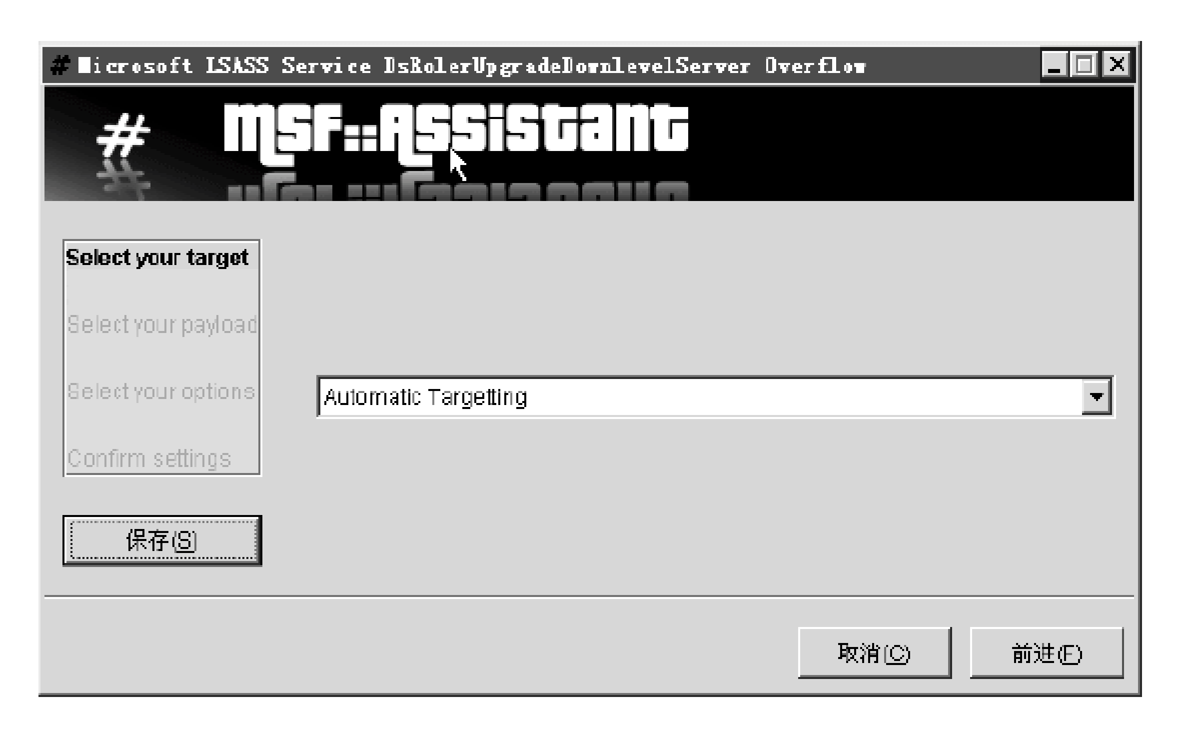



图 4-84　选择漏洞列表相应的参数(1)




图 4-85　选择漏洞列表相应的参数(2)

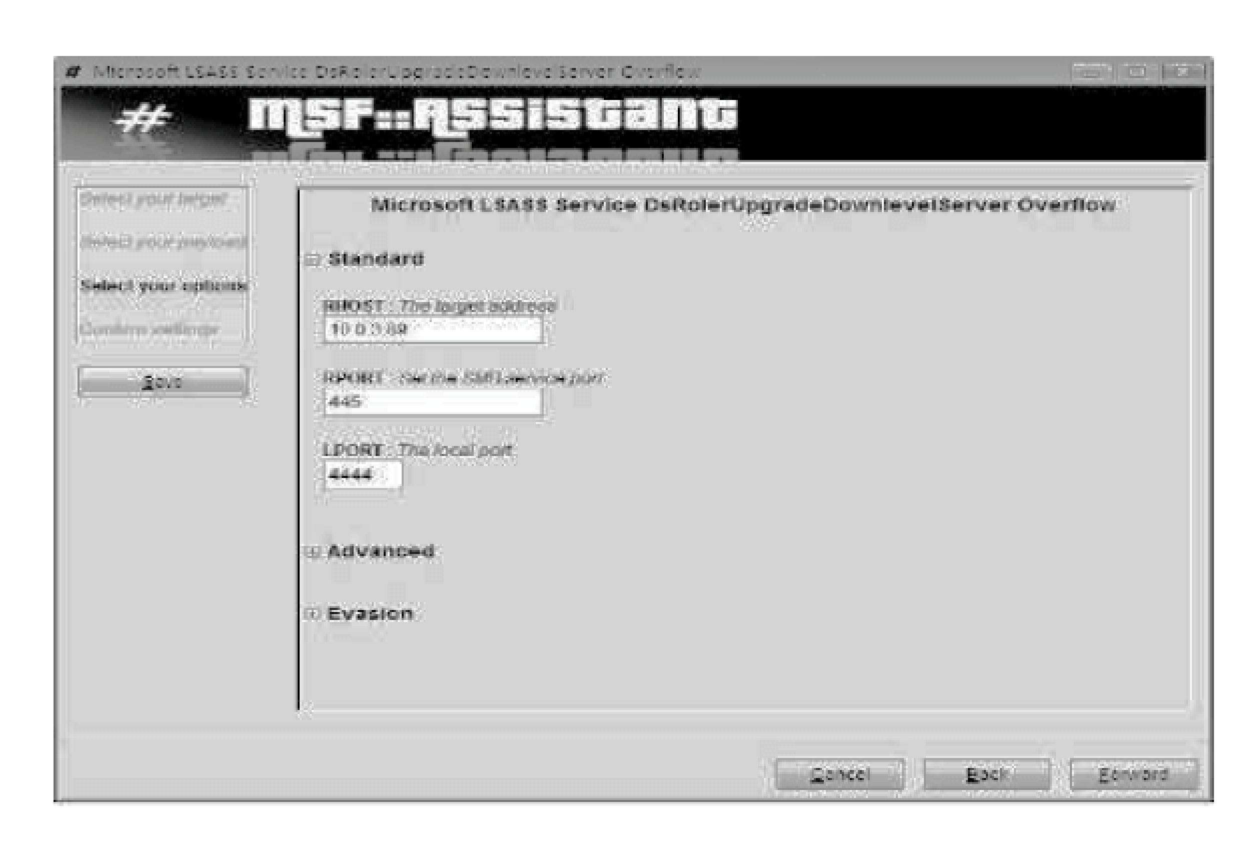



图 4-86　选择漏洞列表相应的参数(3)

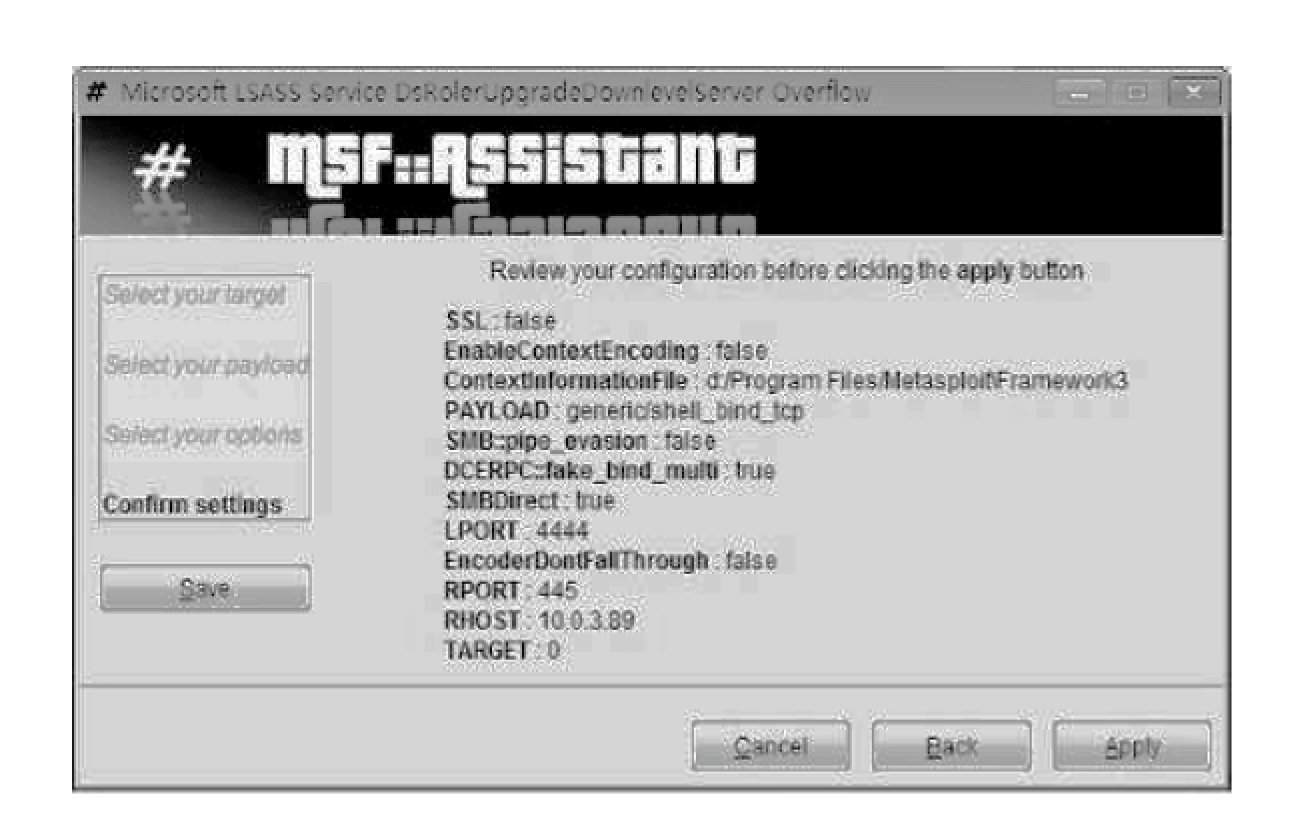



图 4-87　选择漏洞列表相应的参数(4)

在此步时可以单击 Save 按钮保存现有的配置,以便下次使用。

单击 Apply 按钮,则可以开始对被攻击主机使用漏洞进行攻击,在被攻击主机上会出现以下的情形“利用 ms04-011 漏洞导致系统崩溃重启”,如图 4-88 所示。

2）MS06-040

依次选择 exploits-windows-smb,在下面的漏洞列表中双击 ms06_040_netapi,如图 4-89 所示。



图 4-88　对被攻击主机使用漏洞进行攻击

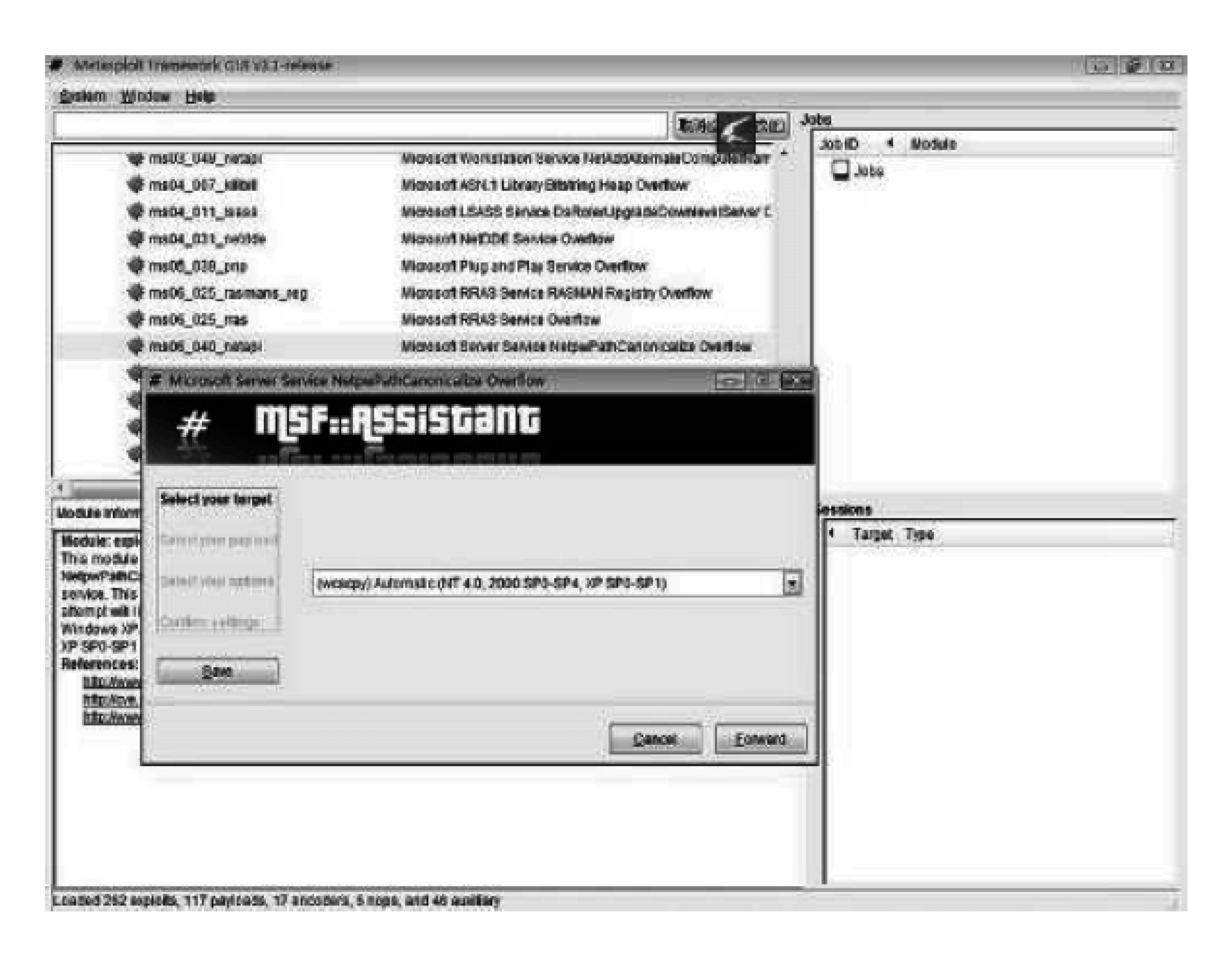


图 4-89　选择漏洞列表

按照下面的步骤在弹出的对话框中选择相应的参数，如图 4-90 所示。

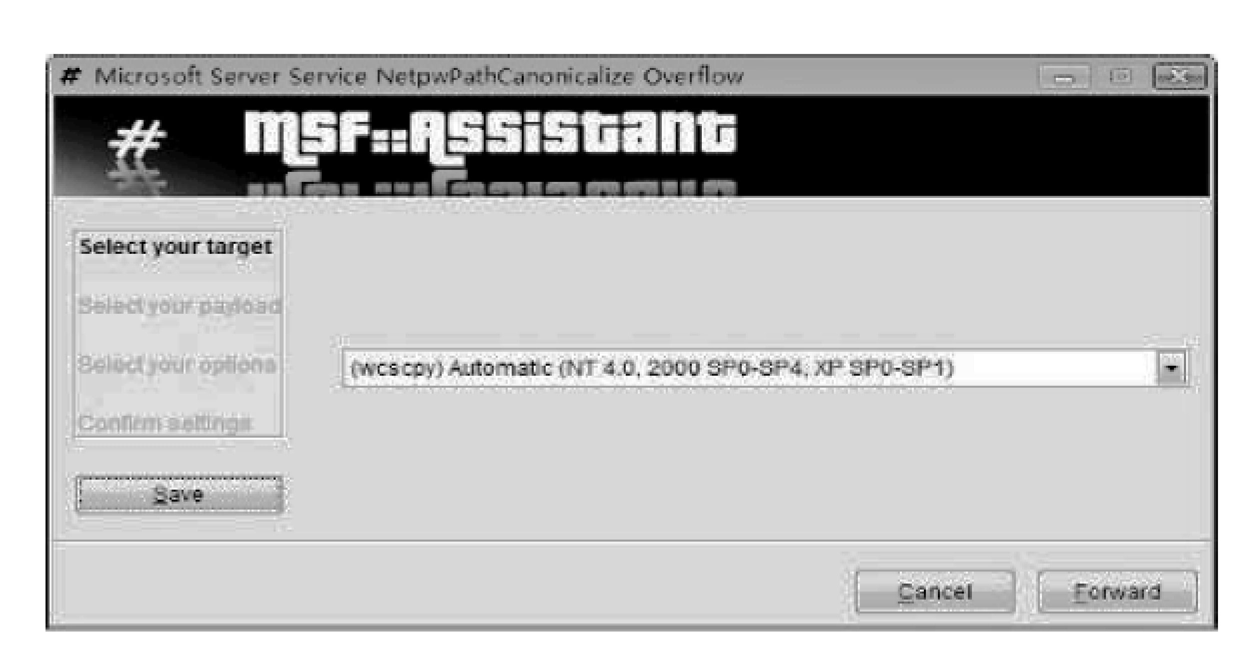



图 4-90　选择相应的参数

在 Select your payload 参数中选择 windows/shell_bind_tcp，如图 4-91～图 4-93 所示。

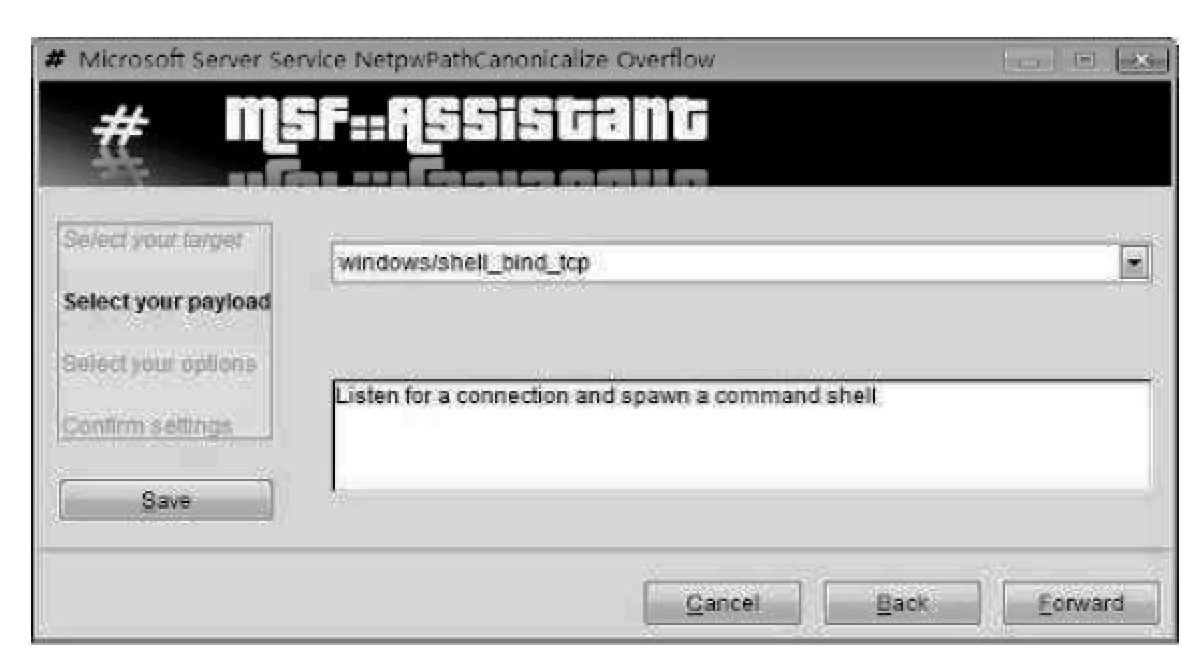



图 4-91　选择漏洞列表相应的参数(1)

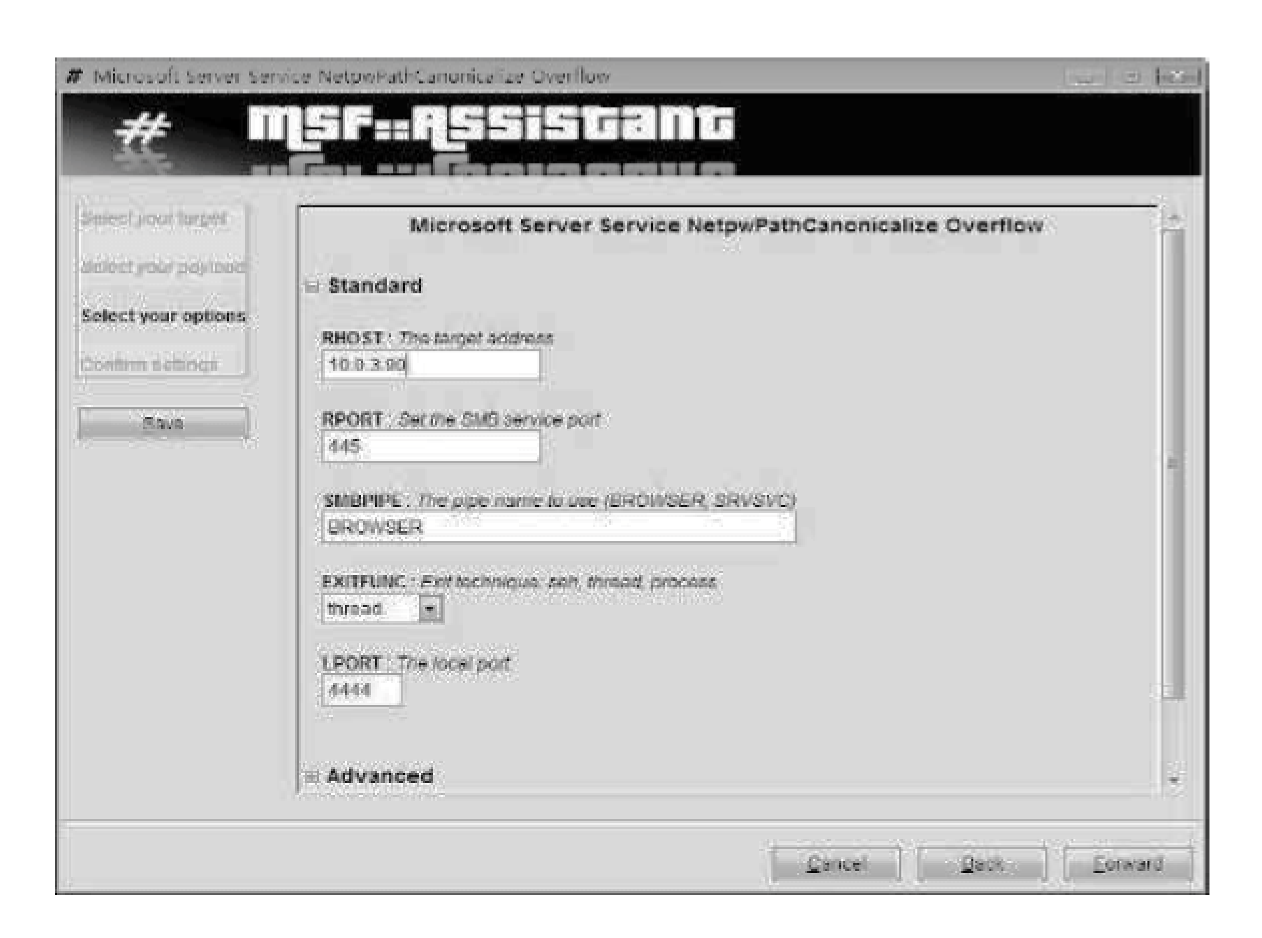



图 4-92　选择漏洞列表相应的参数(2)




图 4-93　选择漏洞列表相应的参数(3)

在此步时可以单击 Save 按钮保存现有的配置，以便下次使用。

单击 Apply 按钮，则可以开始对被攻击主机使用漏洞进行攻击，如果攻击成功，在 metasploit 界面的 sessions 栏中可以看到下图中的内容，双击后即可获得被攻击主机上的 shell(DOS 命令行)，如图 4-94 和图 4-95 所示。

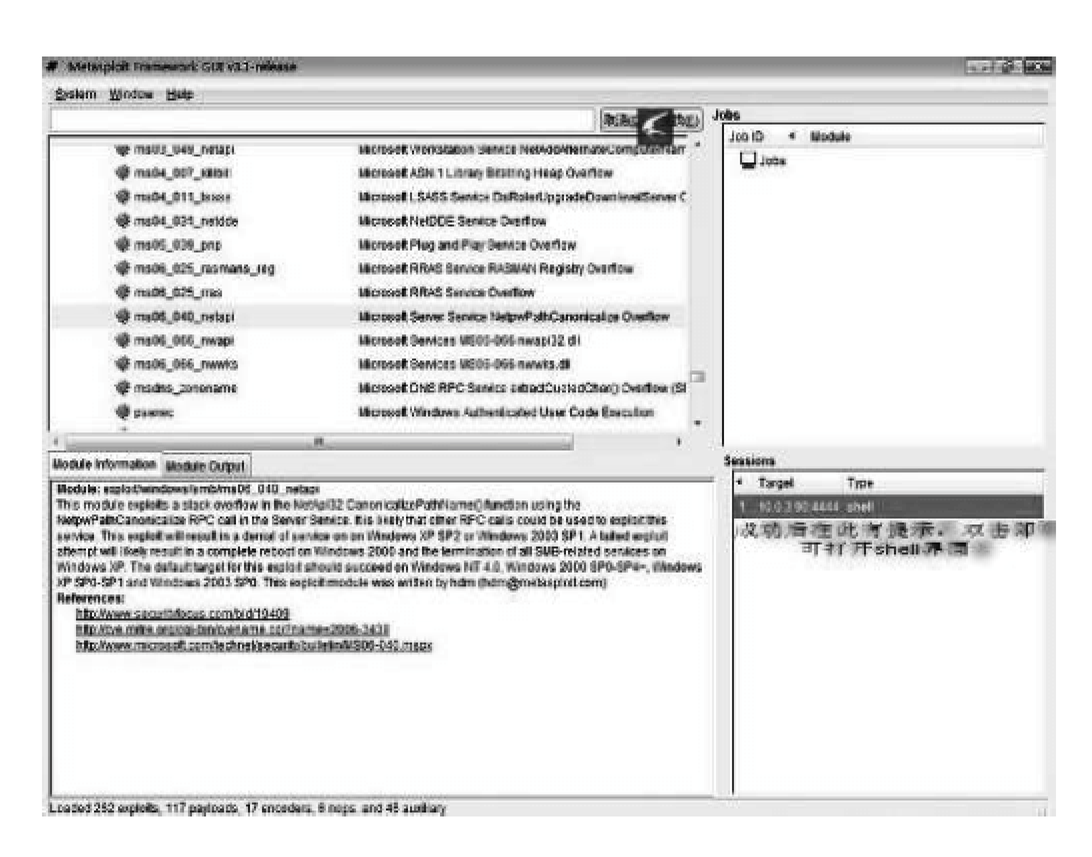


图 4-94 获得被攻击主机上的 shell(1)

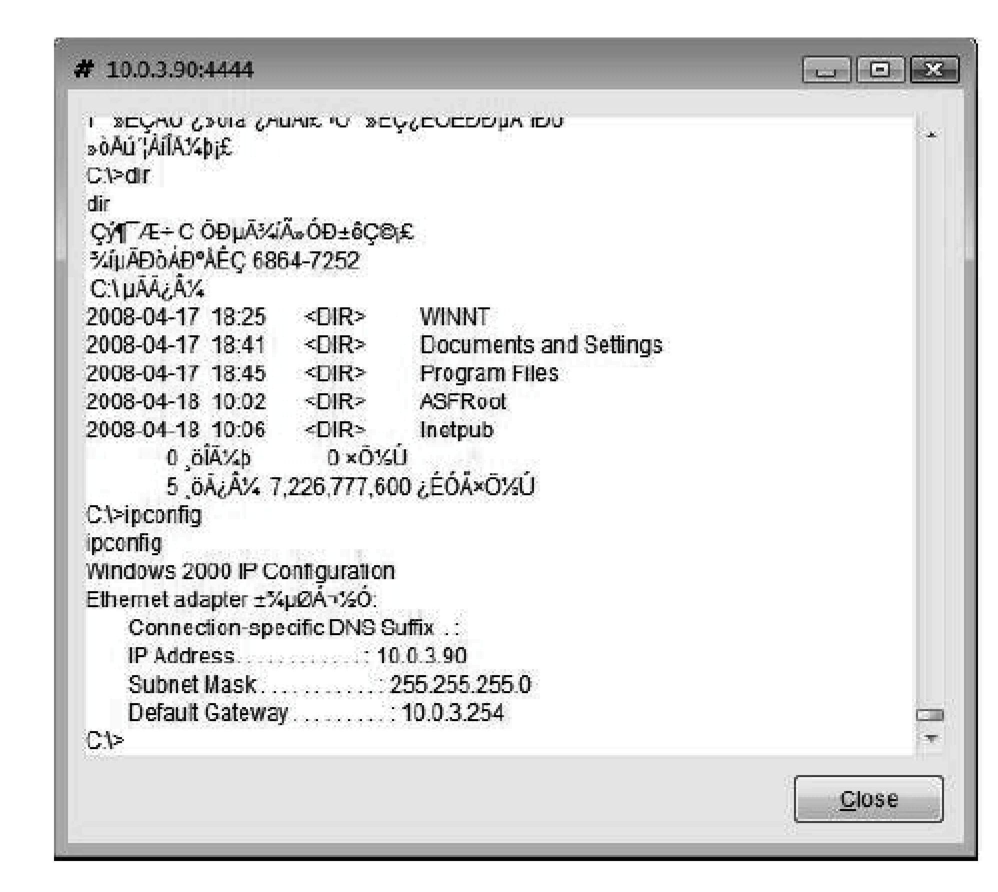



图 4-95 获得被攻击主机上的 shell(2)

在攻击端选择“文件”→“添加主机”选项，添加对方的 IP 地址。

## 3. 查看警报

进入 RG-IDS 控制台，通过“安全事件”组件查看 IDS 检测的安全事件信息，如图 4-96 和图 4-97 所示。

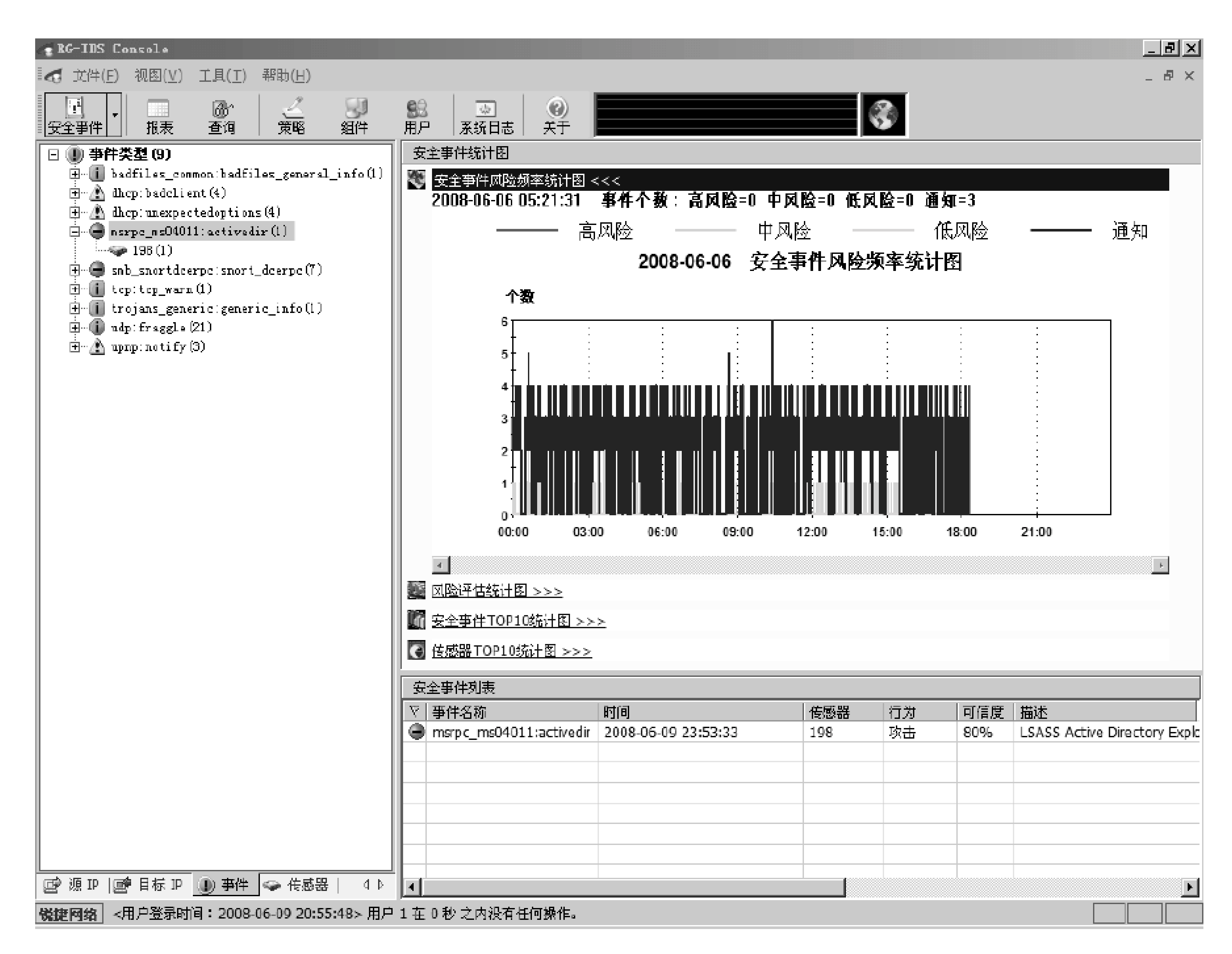



图 4-96 查看 IDS 检测的安全事件信息(1)

RG-IDS 将准确检测出 msrpc:ms04011:activedir_alert 以及 msrpc:ms06040:srvsvc_ms06040_overflow_alert 事件，事件详细信息如图 4-98 和图 4-99 所示。

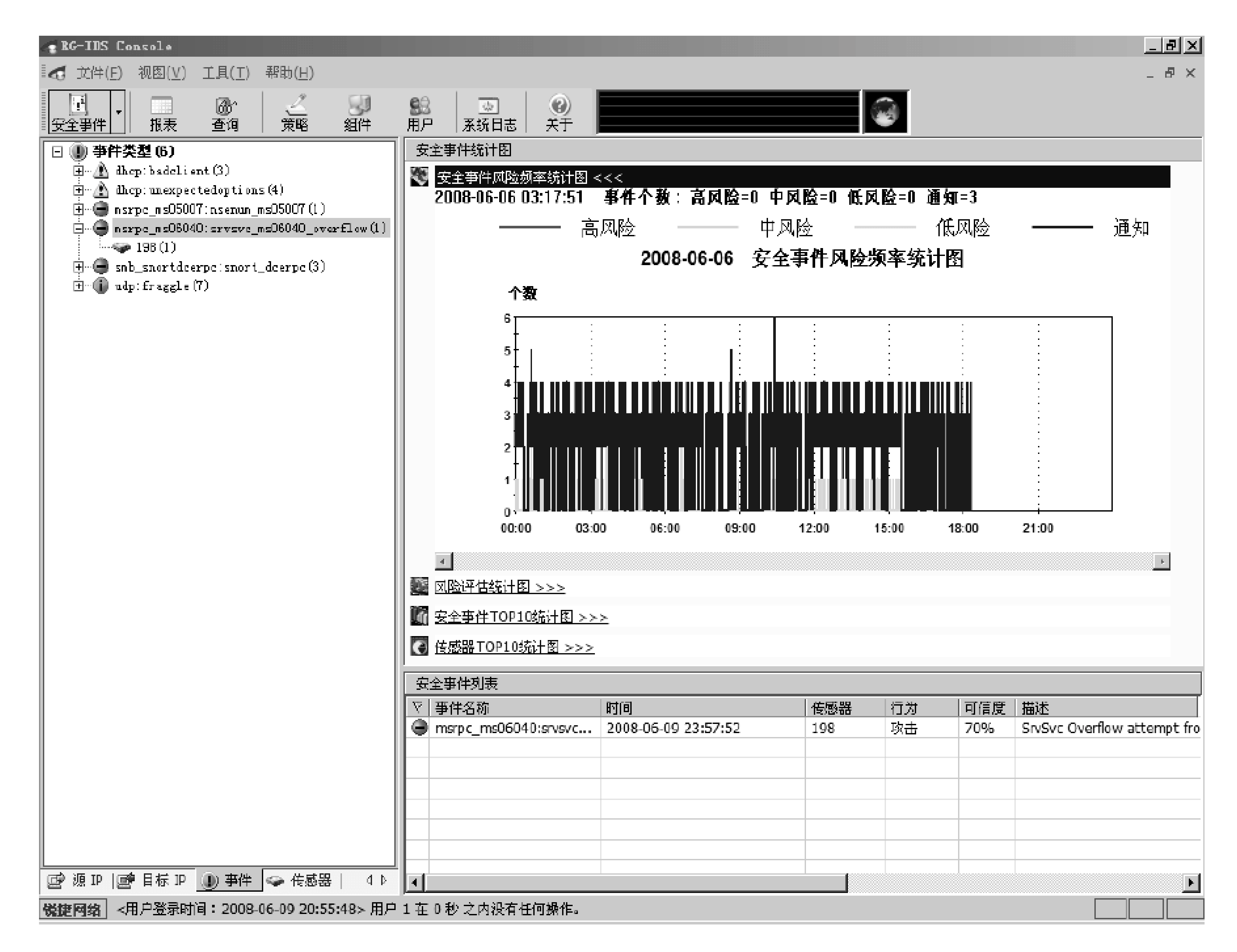



图 4-97　查看 IDS 检测的安全事件信息(2)




图 4-98　事件详细信息(1)




图 4-99　事件详细信息(2)

## 【注意事项】

metasploit 攻击软件只能用于实验。

# 4.11 Windows PnP远程执行代码漏洞攻击检测

## 【实验名称】

Windows PnP 远程执行代码漏洞攻击检测。

## 【实验目的】

使用 RG-IDS 对 MS-05039 Windows PnP(即插即用)远程执行代码漏洞攻击进行检测。

## 【背景描述】

在某网络中发现存在针对 Windows 系统的 MS-05039 攻击，于是网络工程师部署了 IDS 系统对其进行检测。

## 【需求分析】

需求：Microsoft Windows 即插即用(PnP)功能允许操作系统在安装新硬件时能够

检测到这些设备。在 Microsoft Windows 即插即用功能中存在缓冲区溢出漏洞，成功利用这个漏洞的攻击者可以完全控制受影响的系统。

分析：通过 RG-IDS 实时检测和告警，提醒管理员及时安装操作系统补丁，并对遭受攻击的机器进行隔离防御和维护。

## 【实验拓扑】

如图 4-100 所示的网络拓扑，某企业网络管理员发现存在针对 Windows 系统 MS-05039 攻击，于是网络工程师部署 IDS 系统对其进行检测，以实现网络安全防范功能。

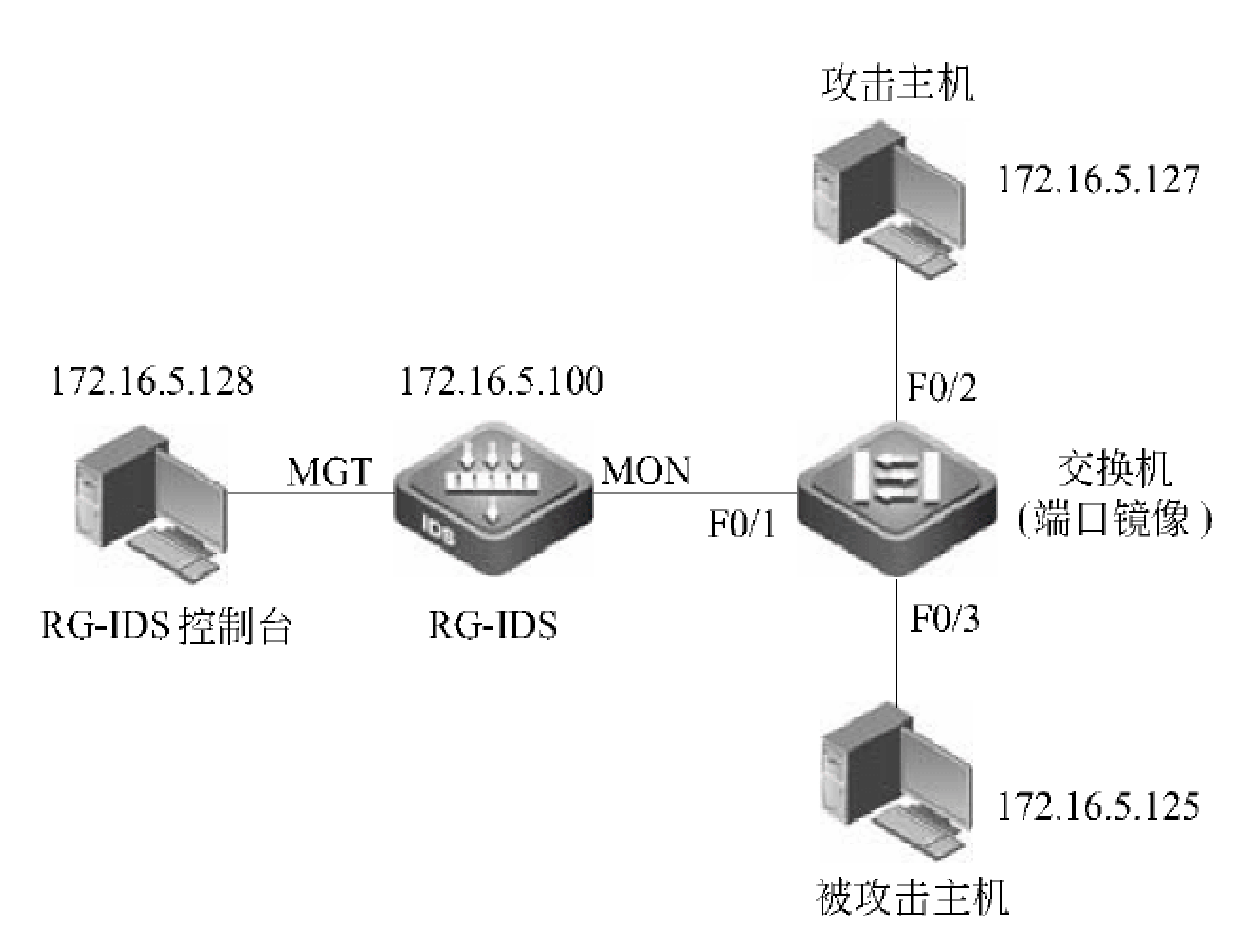



图 4-100 RG-IDS 对远程执行代码漏洞攻击检测拓扑图

## 【实验设备】

| | |
|---|---|
| PC | 3 台 |
| RG-IDS | 1 台 |
| 直连线 | 4 条 |
| 交换机 | 1 台(支持多对一的端口镜像) |
| 攻击软件 | HOD-ms05039-pnp-expl(PnP 即插即用攻击工具) |
| 操作系统 | 未打 MS-05039 补丁的以下任意操作系统(安装在被攻击主机上) |

Microsoft Windows XP SP2

Microsoft Windows XP SP1

Microsoft Windows Server 2003 SP1

Microsoft Windows Server 2003

Microsoft Windows 2000 SP4

## 【预备知识】

- 交换机端口镜像配置。

- RG-IDS 配置。
- HOD-ms05039-pnp-expl 工具使用。

## 【实验原理】

Microsoft Windows 即插即用(PnP)功能允许操作系统在安装新硬件时能够检测到这些设备。

在 Microsoft Windows 即插即用功能中存在缓冲区溢出漏洞,成功利用这个漏洞的攻击者可以完全控制受影响的系统。因为 PnP 服务处理包含了过多数据的畸形消息。在 Windows 2000 上,匿名用户可以利用这个漏洞发送特制消息;在 Windows XP Service Pack 1 上,只有通过认证的用户才能发送恶意消息;在 Windows XP Service Pack 2 和 Windows Server 2003 上,攻击者必须本地登录到系统,然后运行特制的应用程序才能利用这个漏洞。

本实验通过 HOD-ms05039-pnp-expl 工具攻击未打补丁的 Windows 操作系统,使得被攻击系统在一分钟内重启,而 RG-IDS 能及时准确地检测出来并上报控制台。

## 【实验步骤】

### 1. 策略编辑

如图 4-101 所示,单击主界面上的"策略"按钮,切换到策略编辑器界面,从现有的策略模板 For_Windows_Networks 中生成一个新的策略。在新的策略中选择 msrpc:ms05039:upnp_ms05039_alert 签名,并将策略下发到引擎中。

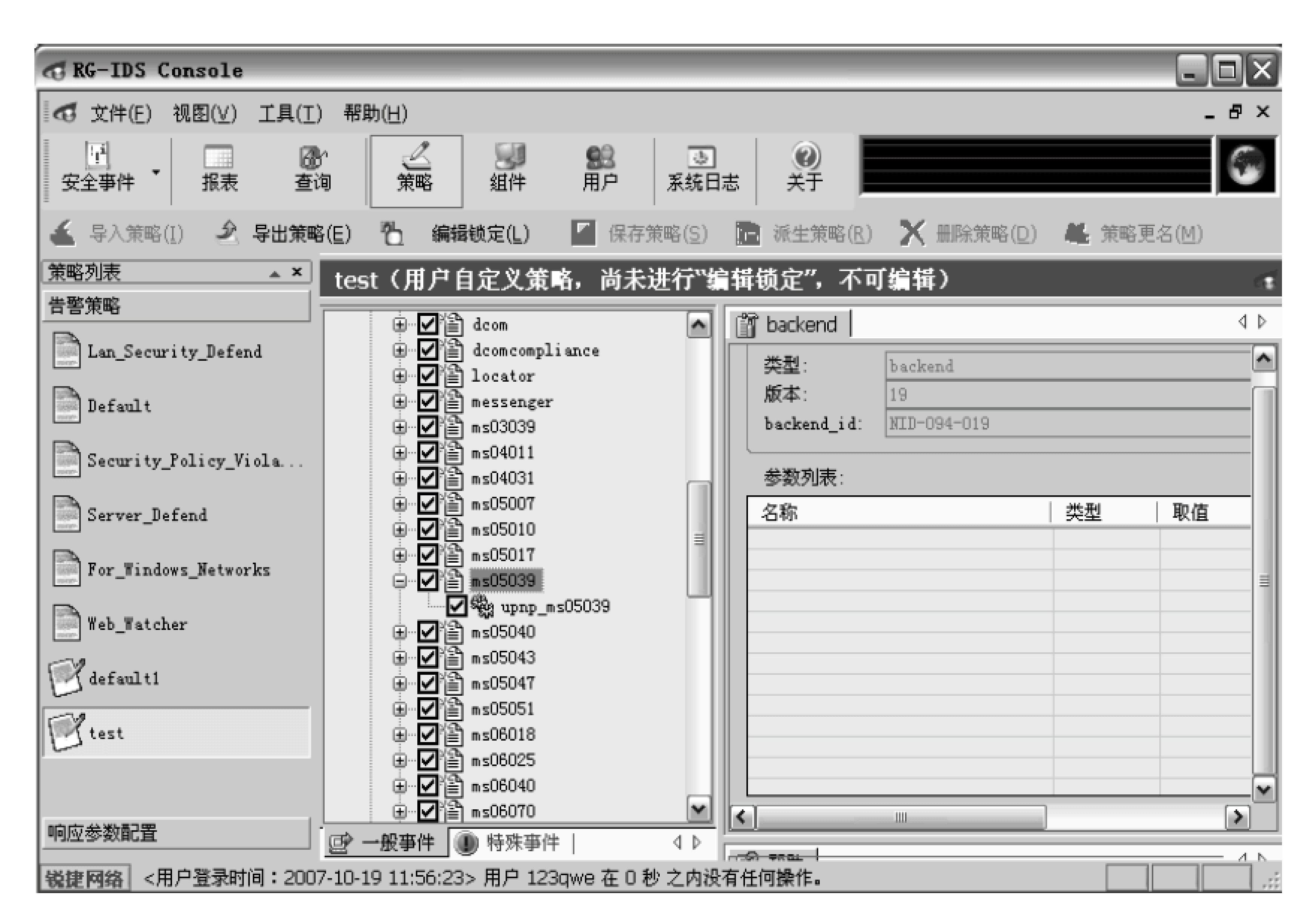



图 4-101 RG-IDS 策略编辑器界面

## 2 实施攻击

将文件 HOD-ms05039-pnp-expl.exe 拖入 DOS 命令行中，如图 4-102 所示。

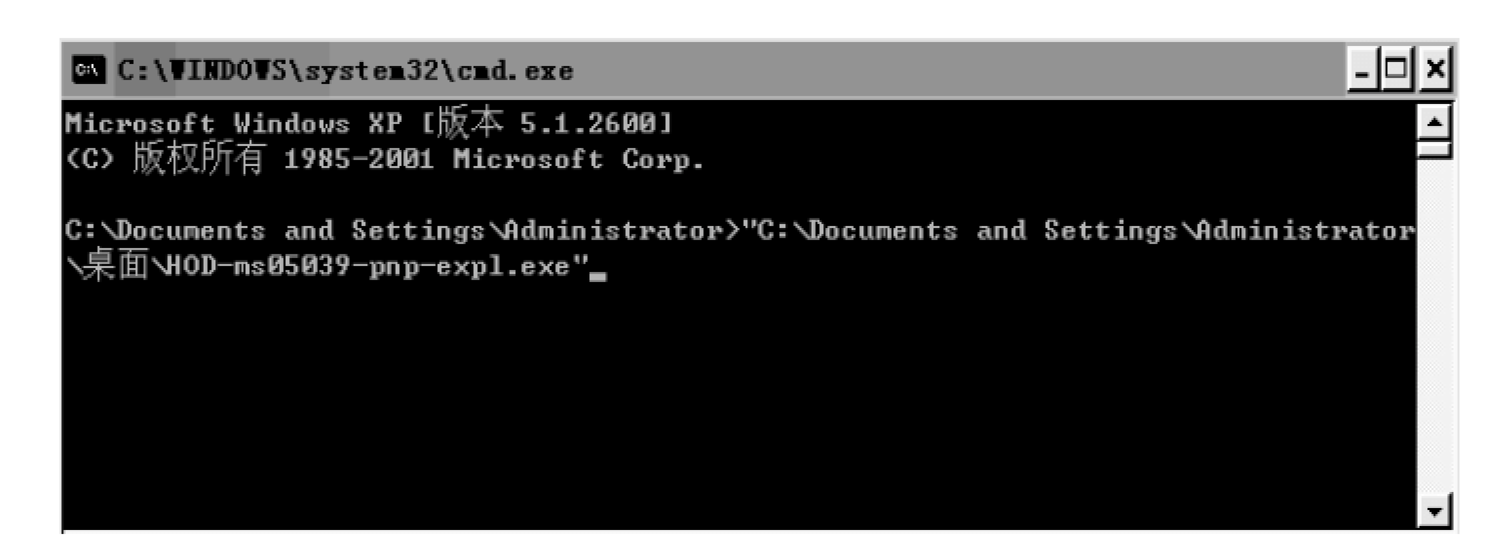



图 4-102　实施攻击

配置攻击参数，在后面加上被攻击的地址 172.16.5.125 和任意端口号，如图 4-103 所示。

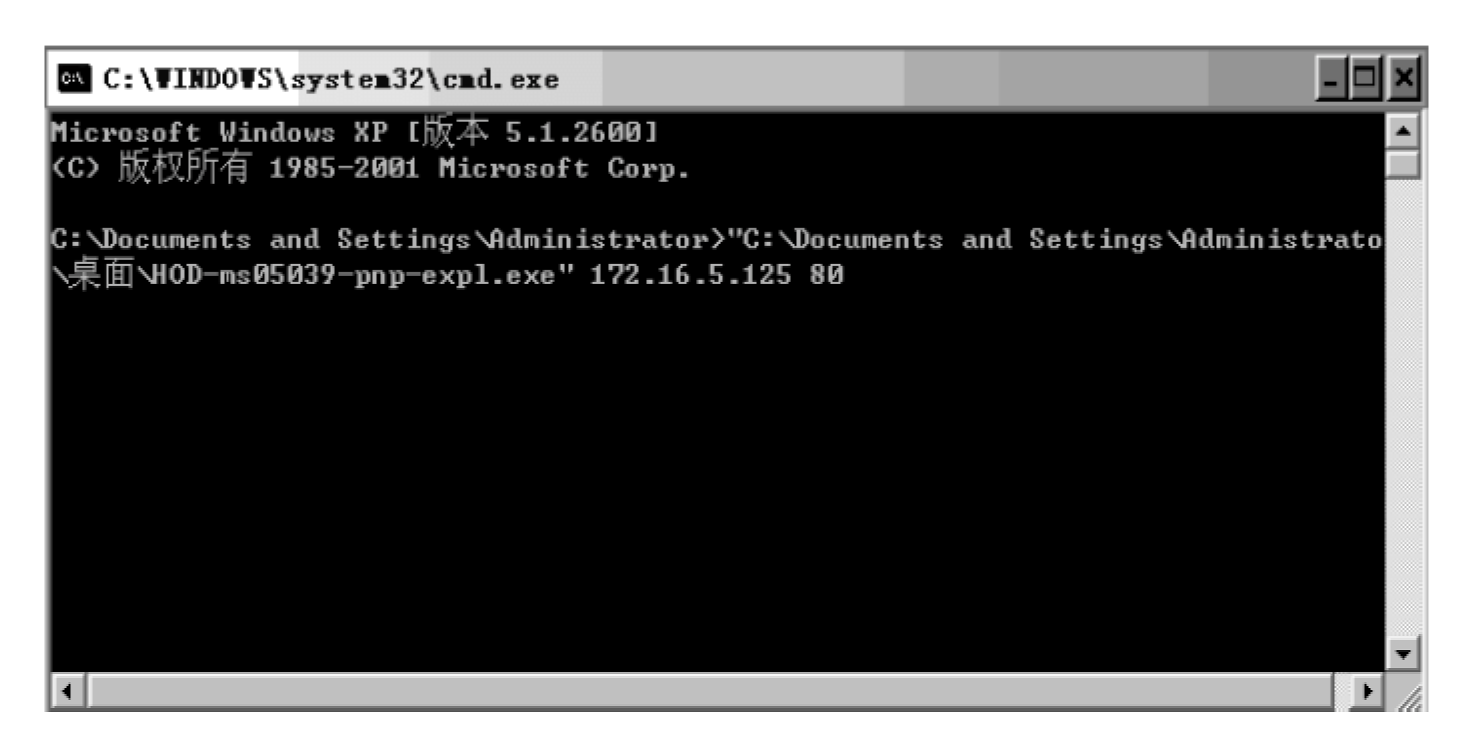



图 4-103　配置攻击参数

攻击完成后，DOS 命令行显示如图 4-104 所示。




图 4-104　DOS 命令行显示

攻击成功后，在被攻击主机 172.16.5.125 系统界面上会弹出提示框，警告系统在 1 分钟后会自动重启，如图 4-105 所示。

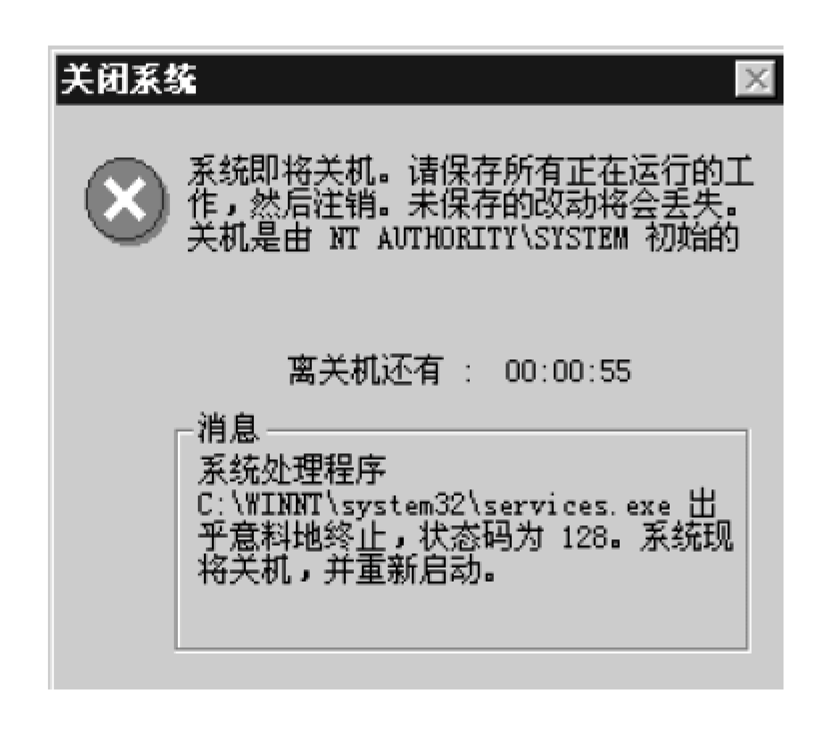



图 4-105　攻击成功后主机的状态

### 3. 查看警报

进入 RG-IDS 控制台，通过“安全事件”组件查看 IDS 检测的安全事件信息，如图 4-106 所示。

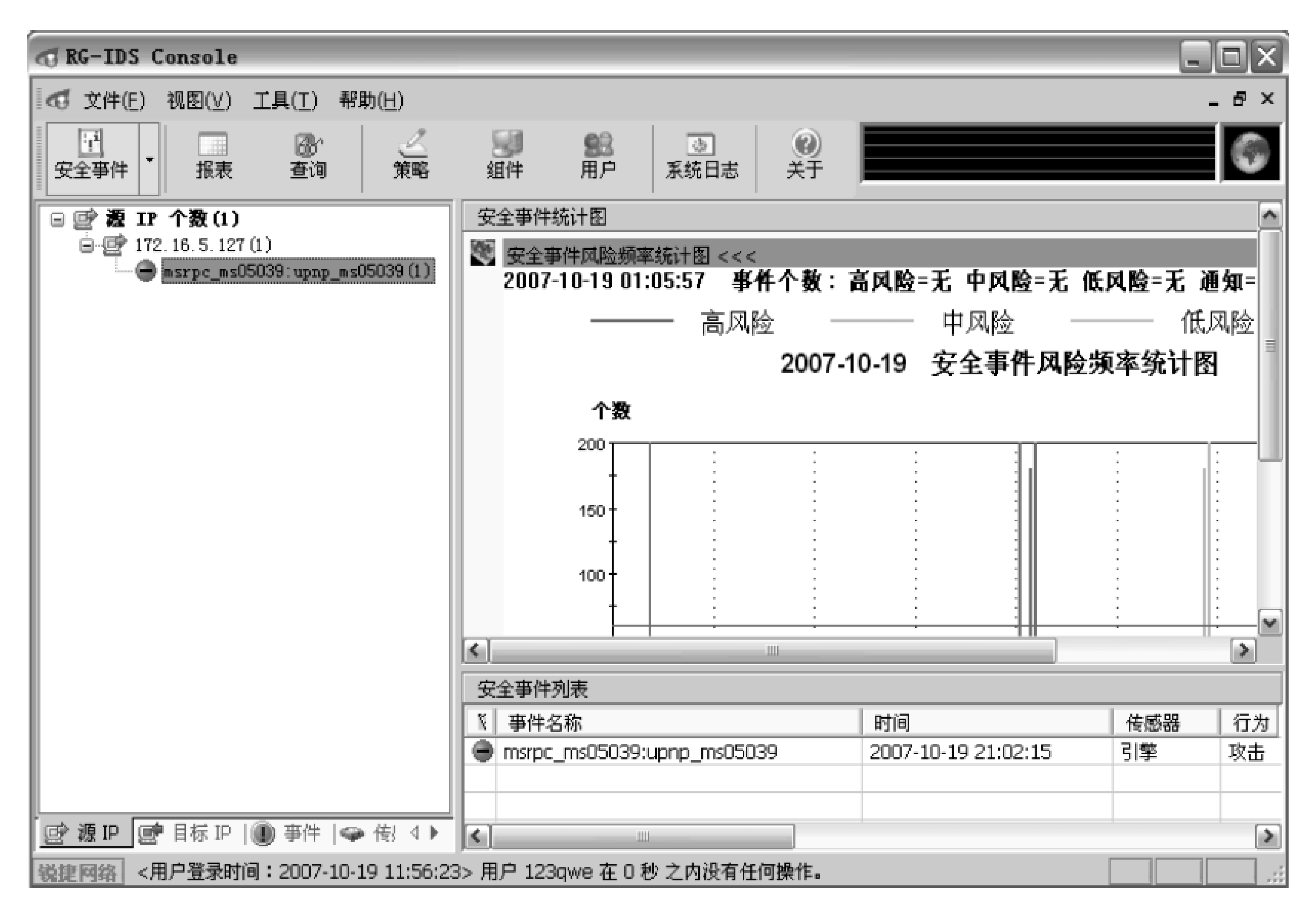



图 4-106　查看 IDS 检测的安全事件信息

RG-IDS 将准确检测出 msrpc:ms05039:upnp_ms05039_alert 事件，事件详细信息如图 4-107 所示。

## 【注意事项】

攻击工具 HOD-ms05039-pnp-expl 只能用于实验。




图 4-107 事件详细信息

# 4.12 木马攻击检测

## 【实验名称】

木马攻击检测。

## 【实验目的】

使用 RG-IDS 对特洛伊木马攻击进行检测。

## 【背景描述】

在某企业网络中，最近发现不少的主机感染了木马，给主机整个网络的正常运行带来了很大影响。

## 【需求分析】

需求：木马，又名特洛伊木马，其名称取自古希腊神话的特洛伊木马记，它是一种基于远程控制的黑客工具，具有很强的隐蔽性和危害性。为了达到控制服务端主机的目的，木马往往要采用各种手段达到激活自己、加载运行的目的。传统的木马分为客户端和服务器端，安装在被攻击主机上的是服务器端，客户端在攻击主机上对被攻击主机进行控制。

分析：通过使用 RG-IDS 进行实时的检测和告警，可以通知管理员在网络中存在木马攻击，并及时地进行查杀。

## 【实验拓扑】

如图 4-108 所示的网络拓扑，某企业网络管理员发现在网络中发现不少主机感染了木马，给主机整个网络的正常运行带来了很大影响，于是部署了 IDS 系统，进行实时的检测和告警，通知管理员网络中存在木马攻击，并及时进行查杀，以实现网络的安全防范功能。

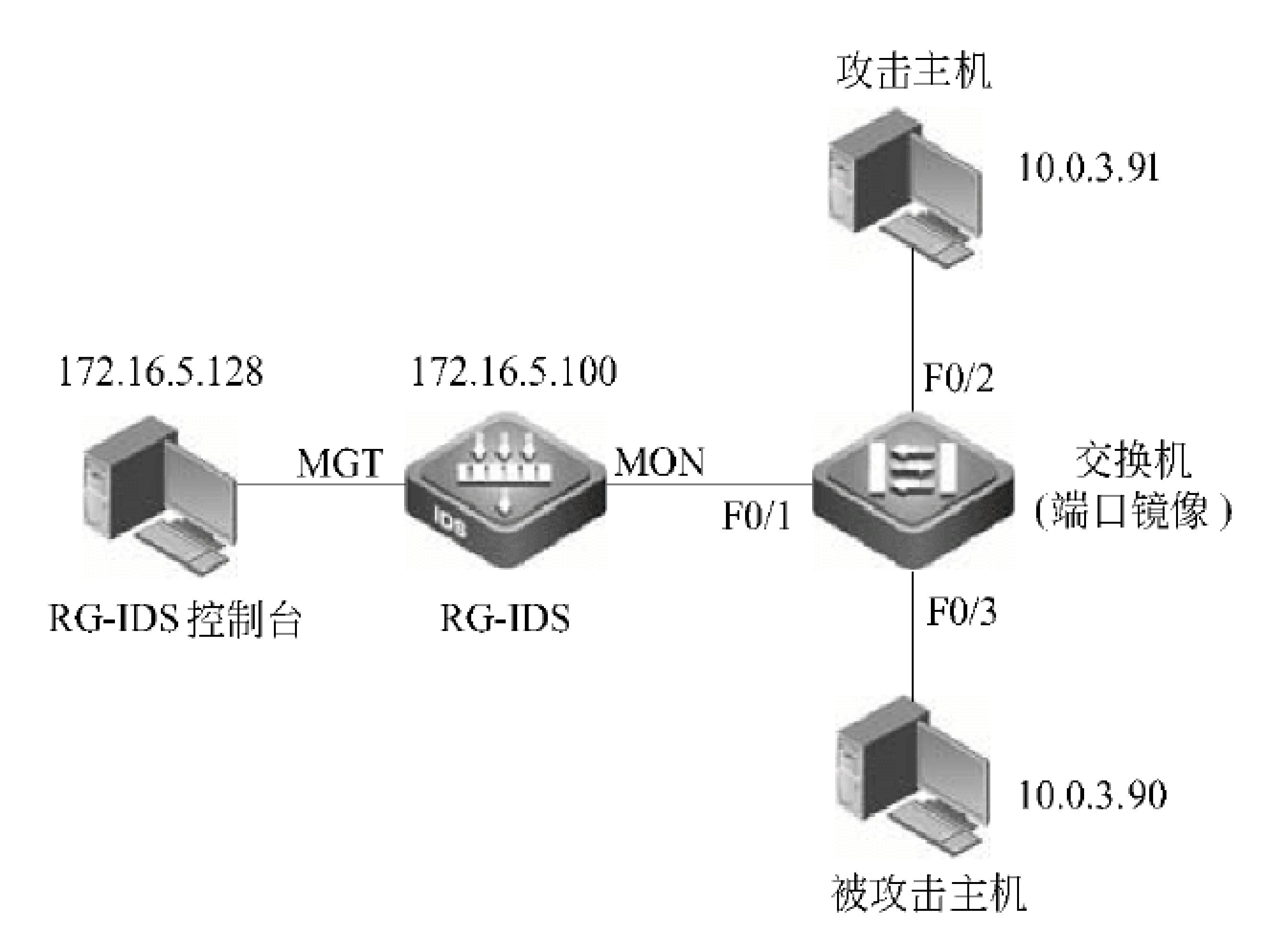



图 4-108　木马攻击检测网络拓扑图

## 【实验设备】

| | |
|---|---|
| PC | 3 台 |
| RG-IDS | 1 台 |
| 直连线 | 4 条 |
| 交换机 | 1 台（必须支持多对一的端口镜像） |
| 攻击软件 | 灰鸽子、冰河 |

## 【预备知识】

- 交换机端口镜像配置。
- RG-IDS 配置。
- 灰鸽子、冰河工具的使用。

## 【实验原理】

灰鸽子是一个国内流行的用于远程控制计算机的程序，时常被恶意使用，普遍被归类为特洛伊木马程序。灰鸽子工作室于 2003 年初成立，定位于远程控制、远程管理、远程监控软件开发，主要产品为灰鸽子远程控制系列软件产品。然而，目前互联网上出现了利用灰鸽子远程管理软件以及恶意破解和篡改灰鸽子远程管理软件为工具的行为。

冰河是一个老牌的木马程序，通过冰河用户可以远程控制被攻击者的主机，具体功能包括：(1)监控目标机屏幕变化，(2)记录各种口令信息，(3)获取系统信息，(4)限制系

统功能，(5)远程文件操作，(6)注册表操作等。

RG-IDS 通过检测这两种木马运行时的网络行为特征，并对其防御。

## 【实验步骤】

### 1. 策略编辑

如图 4-109 所示，单击主界面上的“策略”按钮，切换到策略编辑器界面，从现有的策略模板中生成一个新的策略。在新的策略中选择 trojans：huigz：. huigz_alert 以及 trojans：glactcp：glac_tcp_alert 签名，并将策略下发到引擎中。

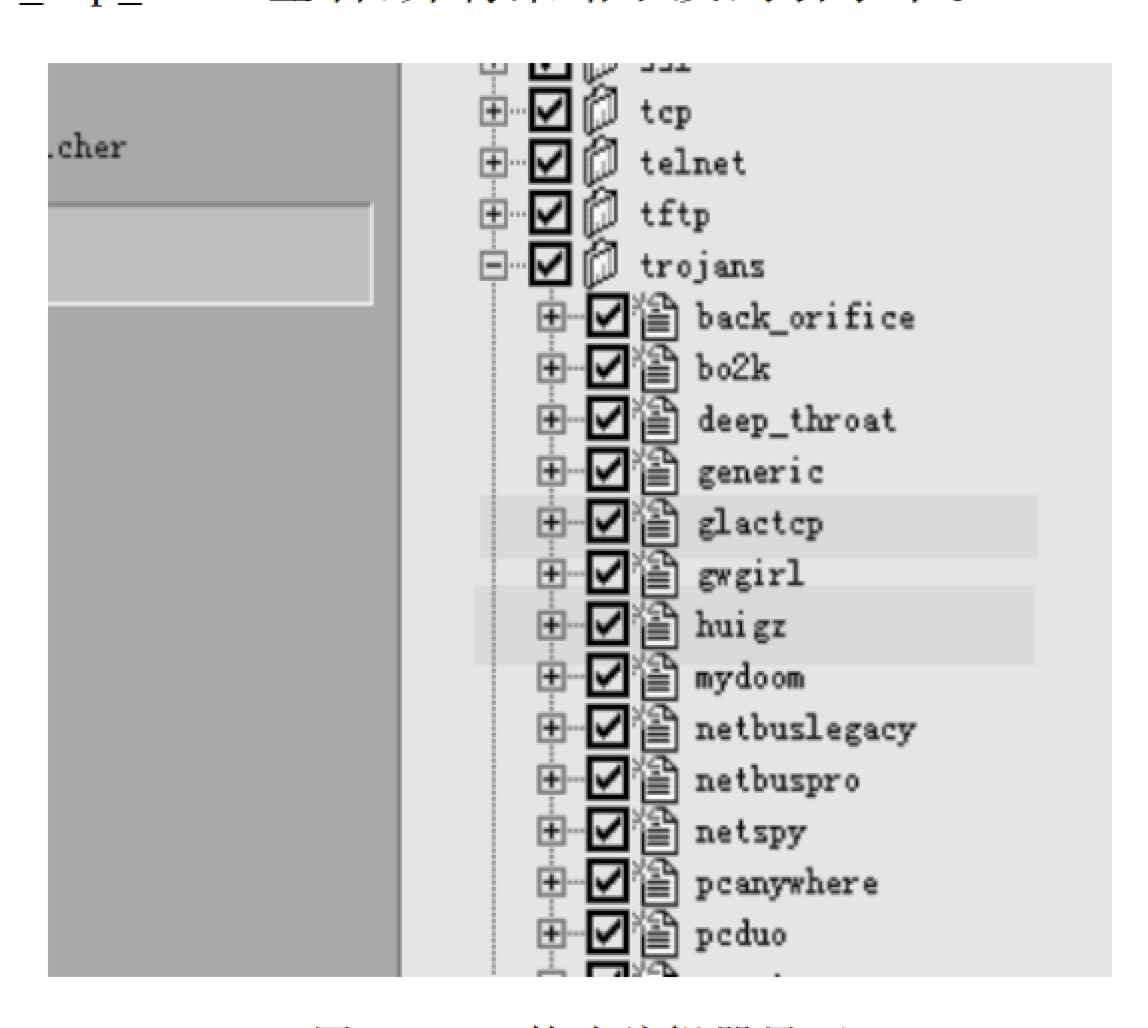



图 4-109　策略编辑器界面

### 2 实施攻击

1）灰鸽子木马

双击灰鸽子客户端 H_Client. exe（在本案例中如果灰鸽子客户端无法打开，请重新解压“灰鸽子_牵手. zip”文件，生成一个新的客户端程序再执行），如图 4-110 所示。

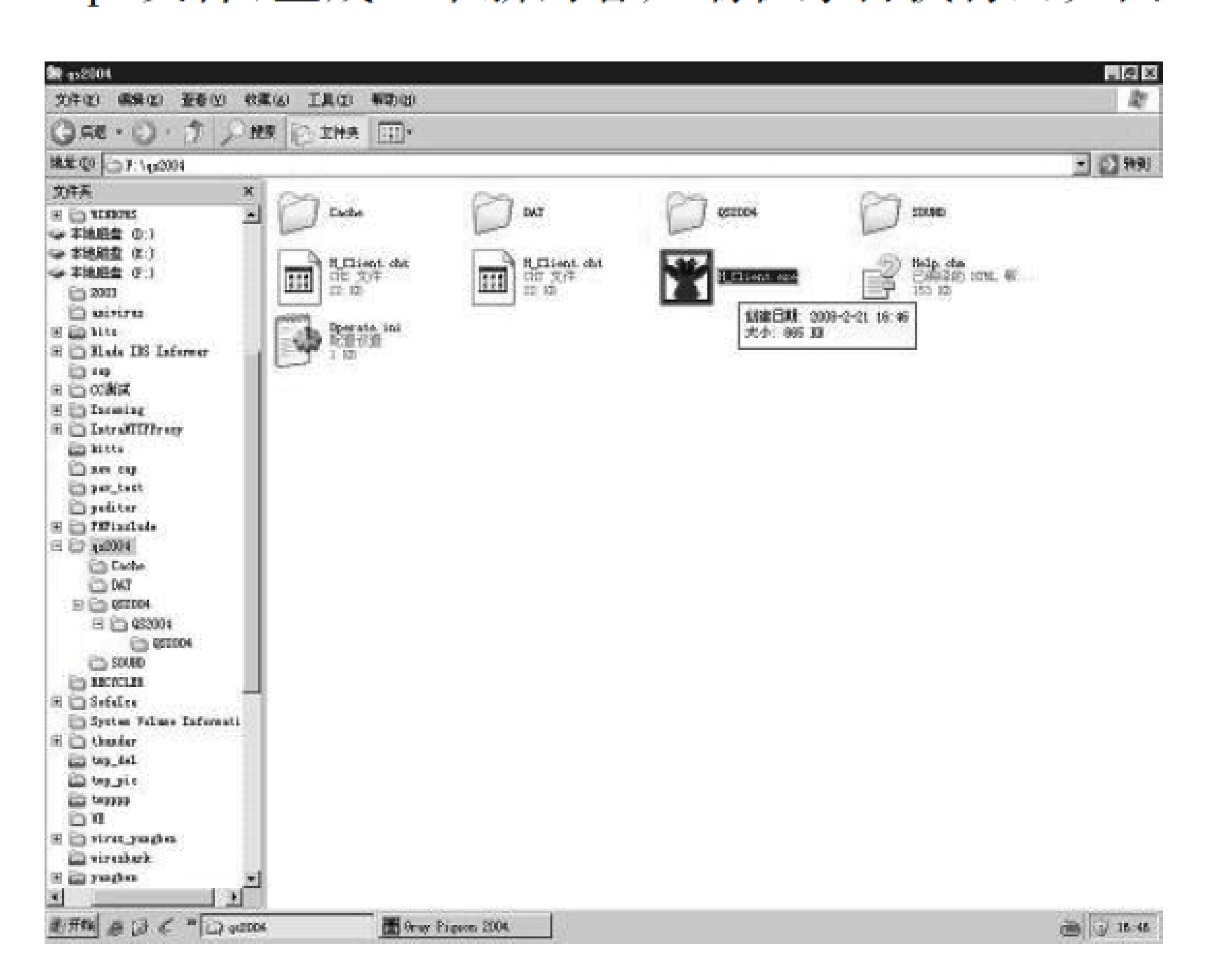


图 4-110　打开灰鸽子木马程序

选择“文件”菜单下的“配置服务程序”选项或直接按 F12 键进入服务器端并进行配置，如图 4-111 所示。

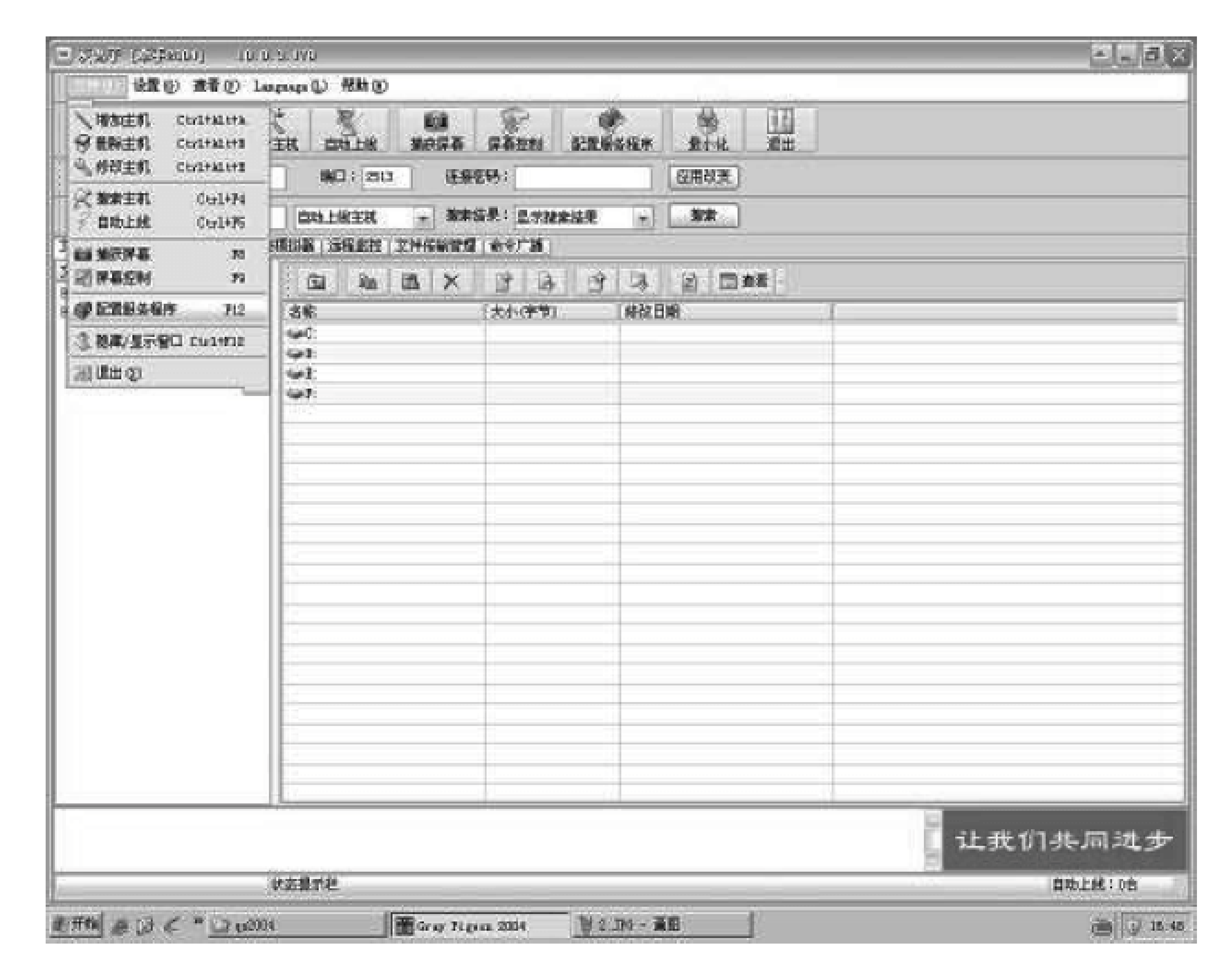



图 4-111　选择配置服务程序

在“连接类型”选项卡中默认选择“主动连接型：远程打开监听端口，等待你的连接控制”单选按钮，其他设置均可按默认无须修改，单击“生成服务器”按钮，如图 4-112 所示。




图 4-112　选择主动连接型

服务器端程序 Setup.exe 就生成了，如图 4-113 所示。

把服务器端程序 Setup.exe 复制到被攻击主机上并双击运行服务器端程序 Setup.exe，如图 4-114 所示。

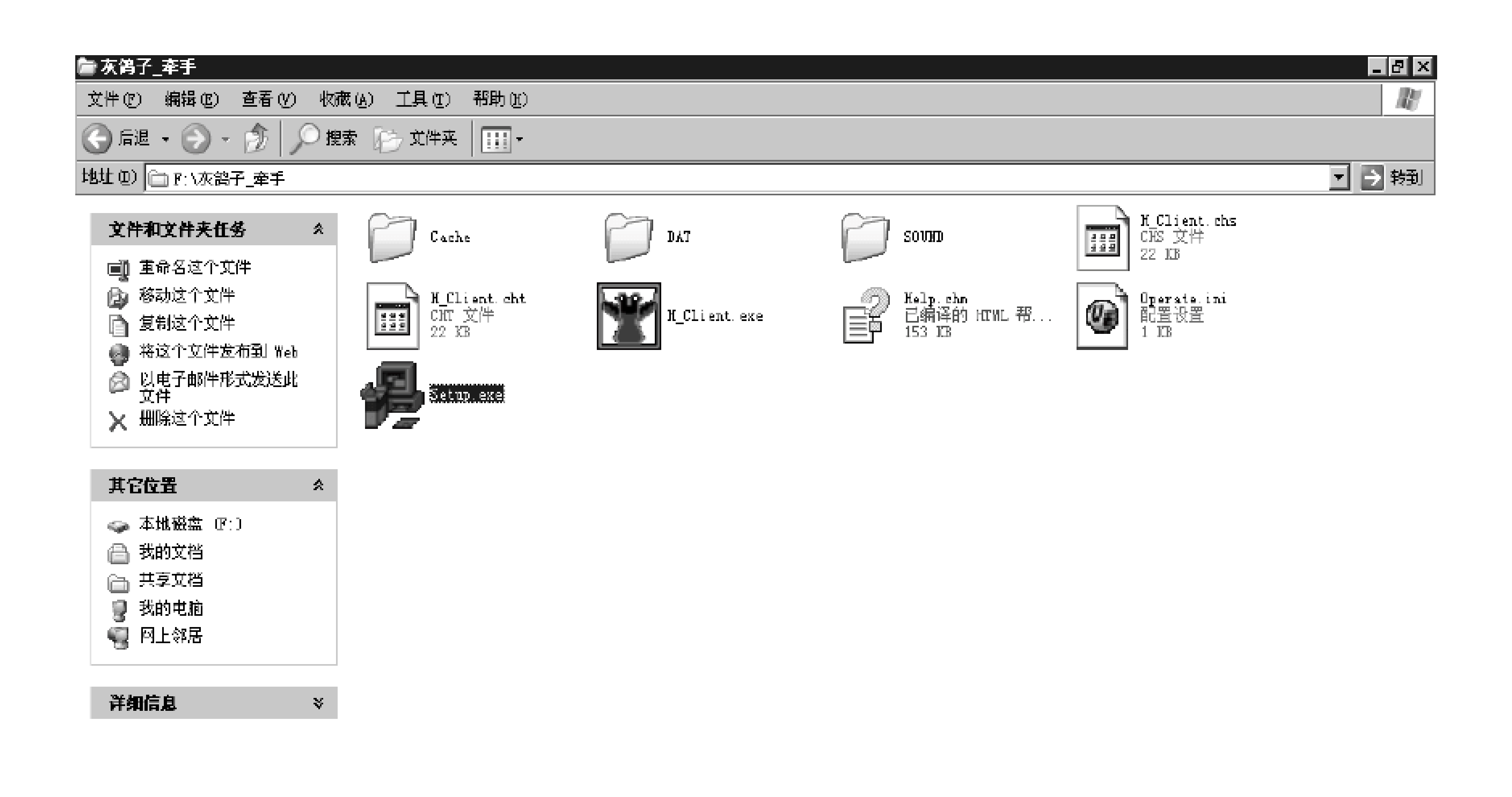


图 4-113　生成服务器端程序

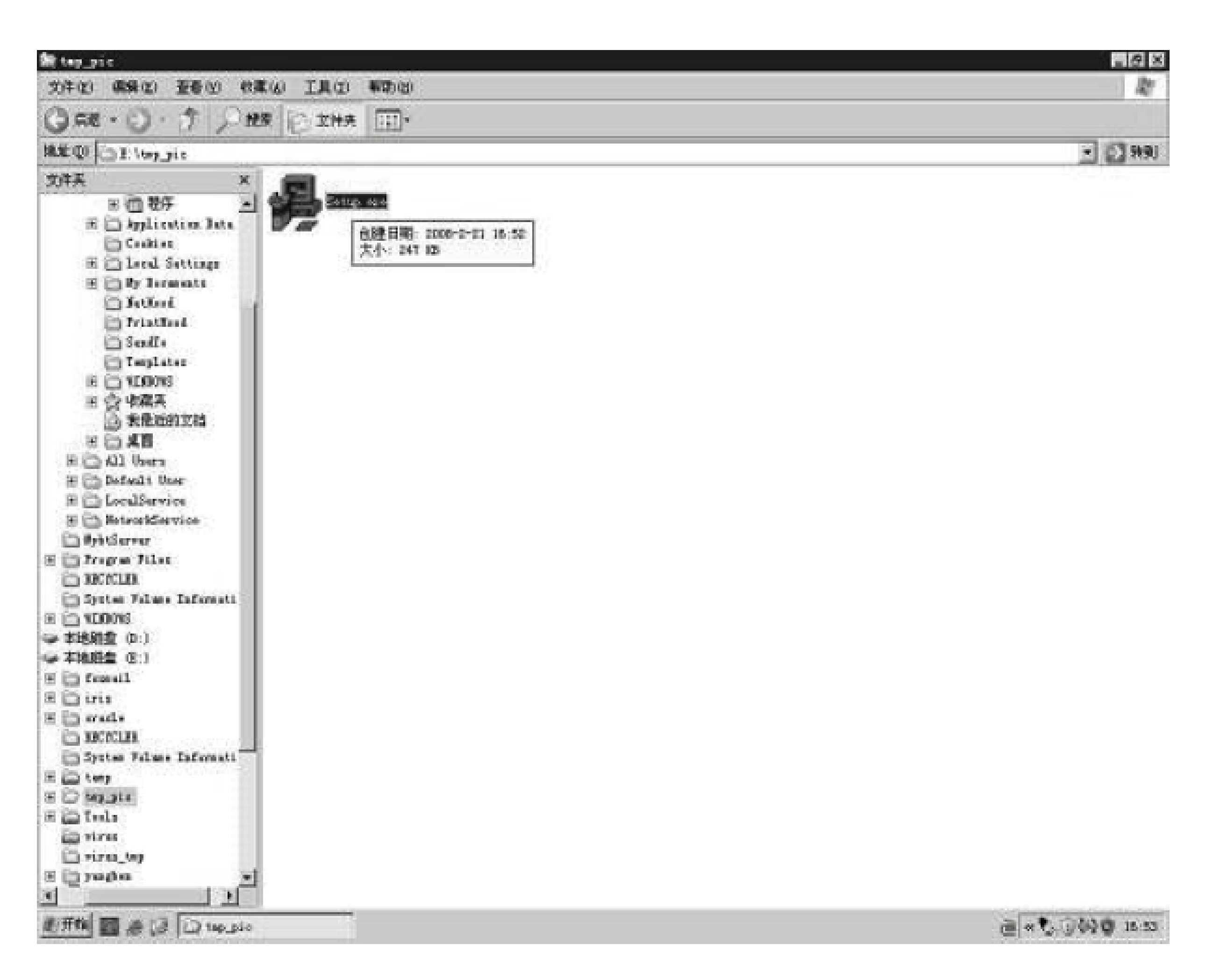


图 4-114　复制服务器端程序

在客户端 H_Client.exe 上单击“增加主机”按钮，添加对方的(运行了灰鸽子服务器端的被攻击主机)IP 地址，如图 4-115 所示。

此时可进行一系列操作，如查看对方系统信息、下载对方文件到本地等，如图 4-116 和图 4-117 所示。

2) 冰河木马

双击冰河客户端 G_CLIENT.EXE，并选择“设置”→“配置服务器程序”选项(注：冰河木马跟上文所提的灰鸽子木马不一样，服务器端程序 G_SERVER.EXE 并不是随着配置生成的，以下步骤只是改变其属性而已。原始的服务器端程序 G_SERVER.EXE 必

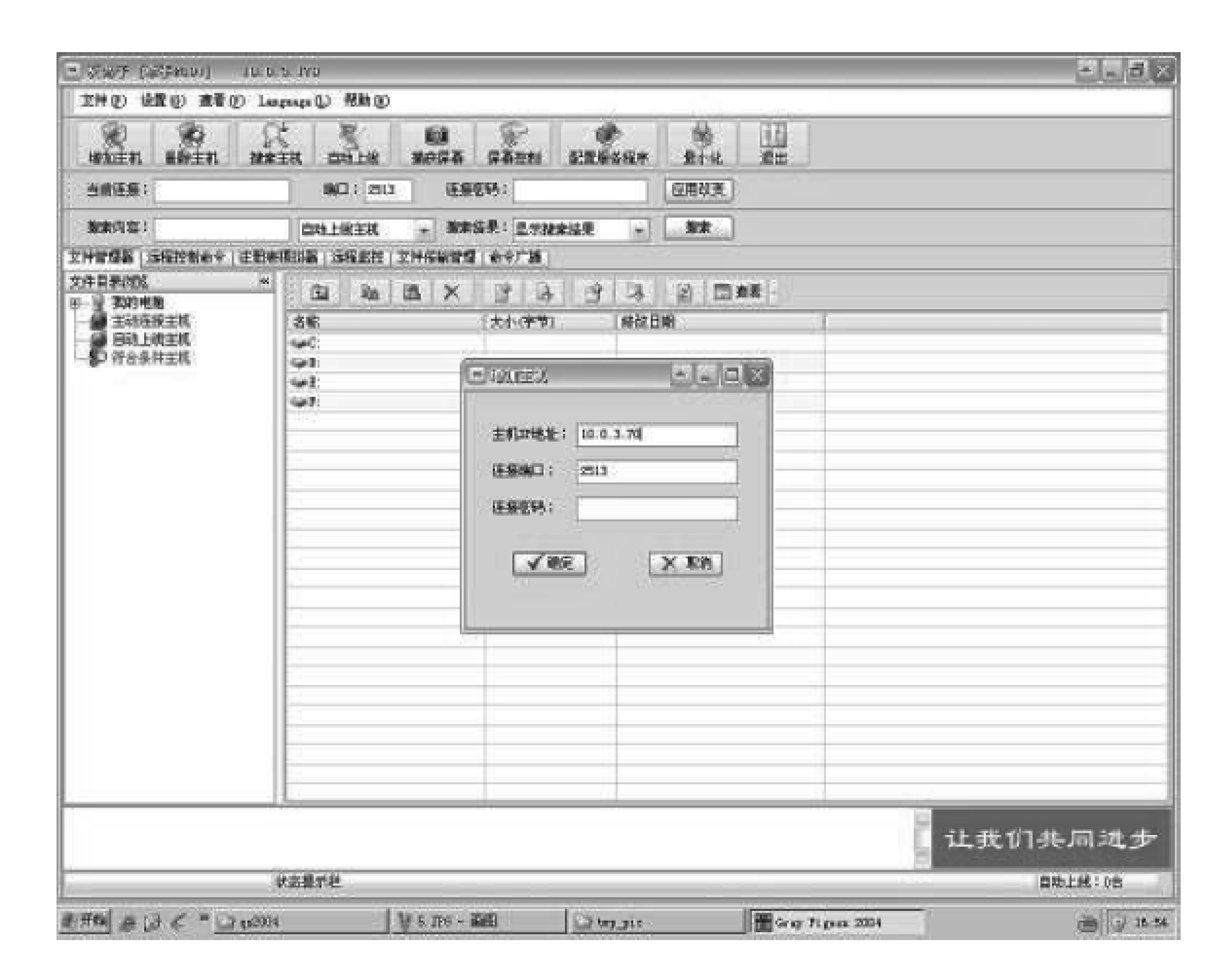


图 4-115　添加对方的 IP 地址

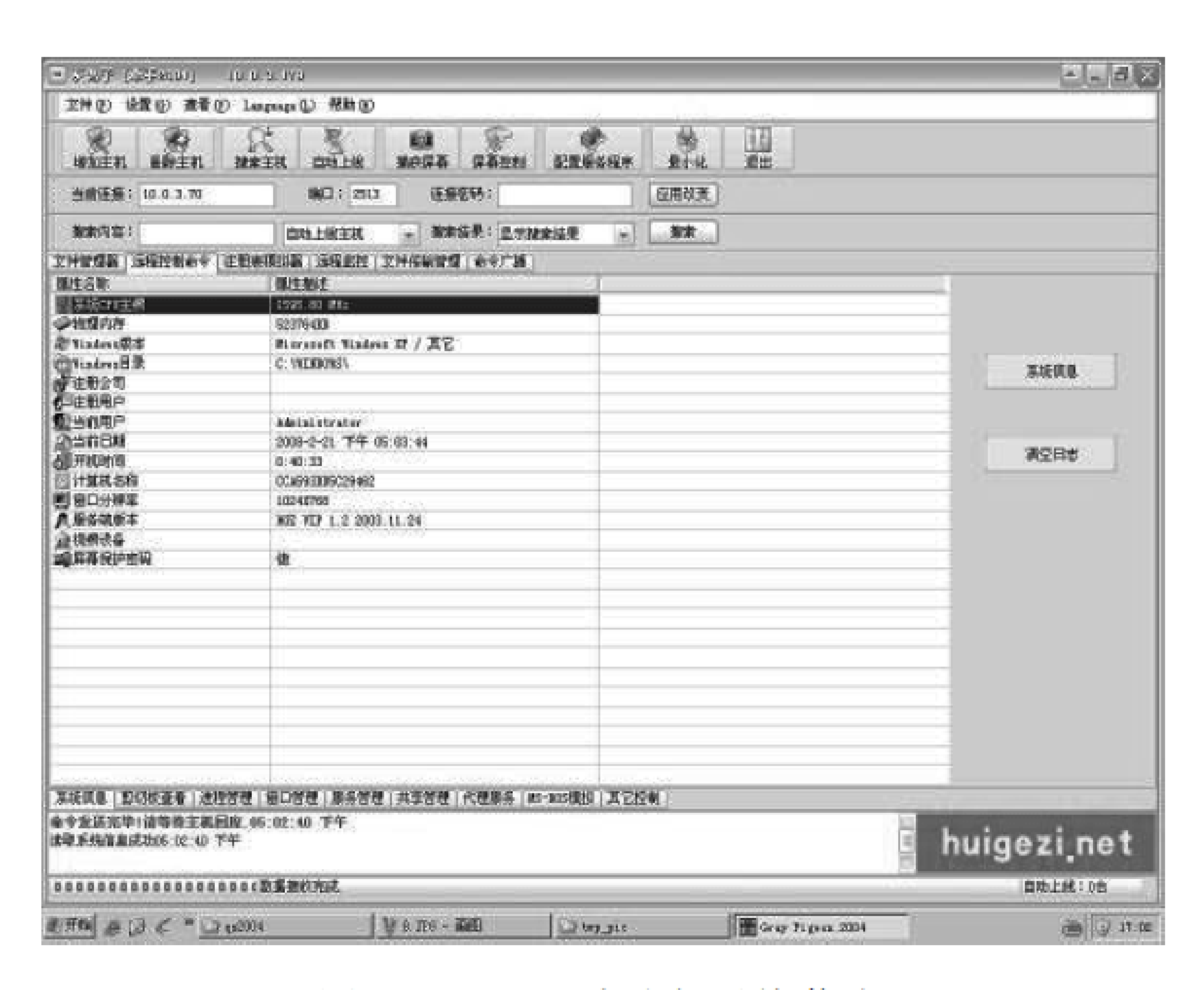


图 4-116　查看对方系统信息

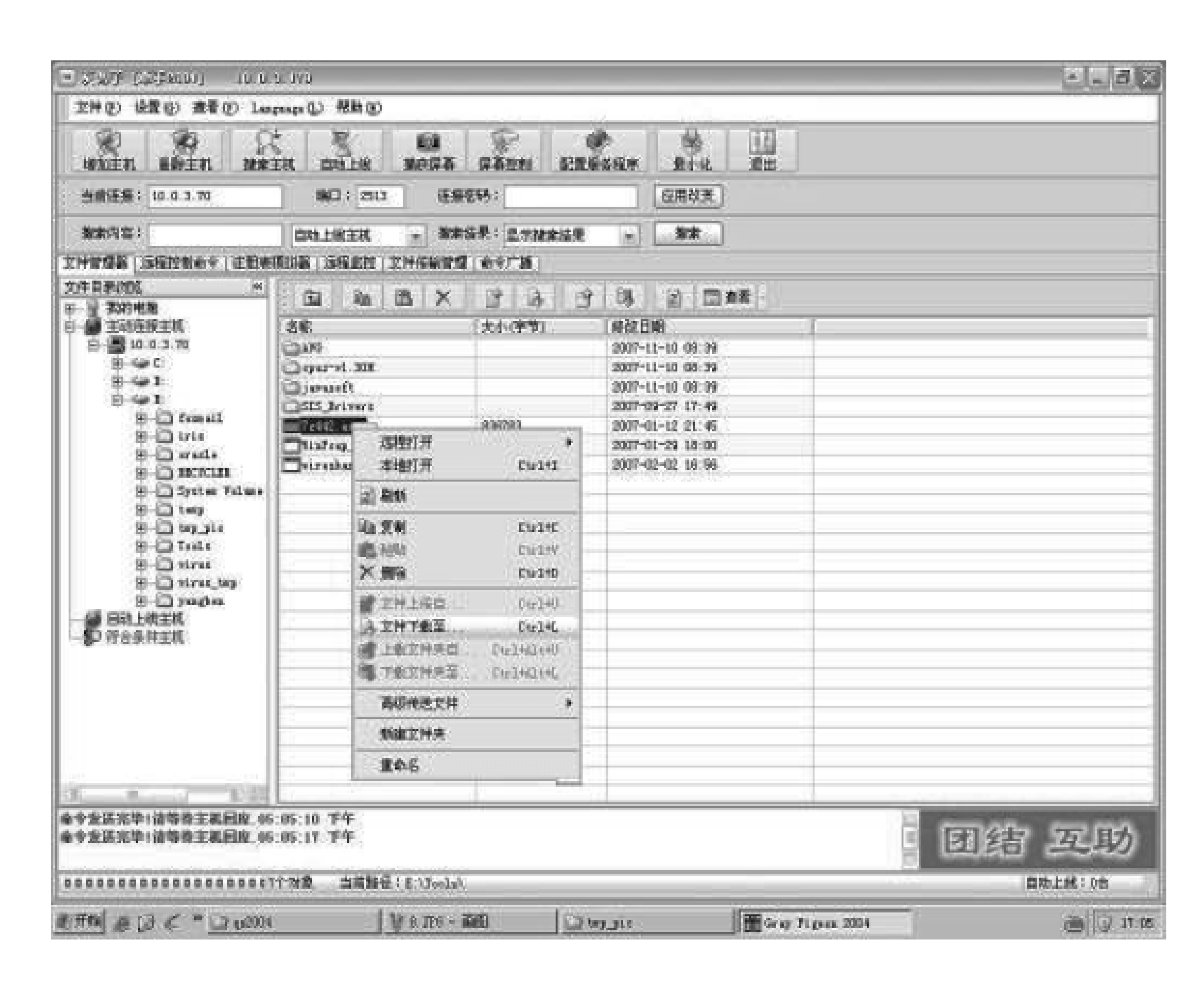


图 4-117　下载对方文件到本地

须跟客户端程序 G_CLIENT.EXE 在同一文件夹下，否则无法完成配置），如图 4-118 所示。




图 4-118　配置服务器程序(1)

按照默认设置无须改变参数，单击“确定”按钮，如图 4-119 所示。




图 4-119　配置服务器程序(2)

所有配置均确认无误后再单击“是”按钮，如图 4-120 所示。

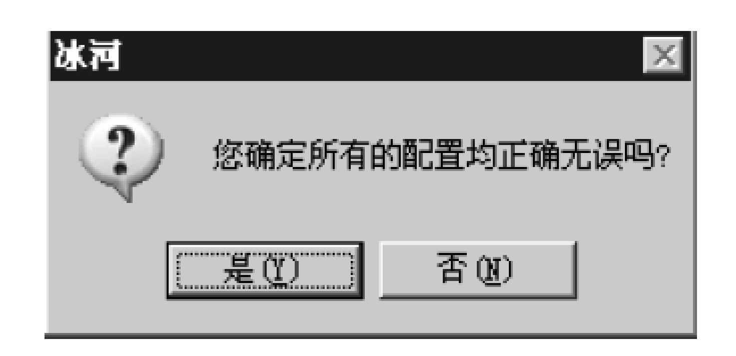



图 4-120　提示信息框

单击“关闭”按钮，完成服务器配置，如图 4-121 所示。

服务器端程序 G_SERVER.EXE 配置就生效了，如图 4-122 所示。

把冰河服务器端 G_SERVER.EXE 复制到被攻击主机上并双击运行服务器端程序 G_SERVER.EXE。




图 4-121　完成服务器配置

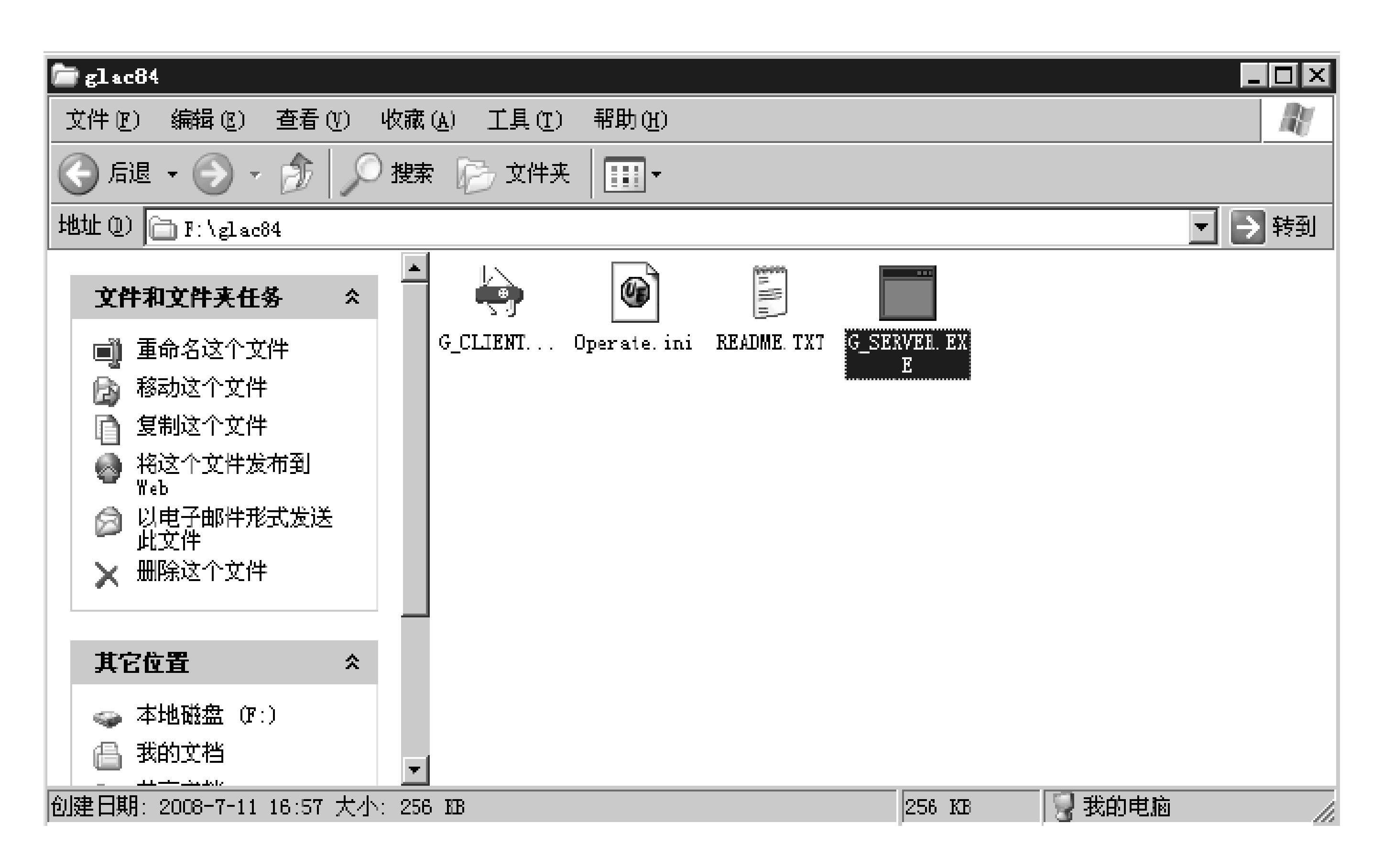



图 4-122　生成服务器端程序

在攻击主机上的冰河客户端 G_CLIENT.EXE 上选择“文件”→“添加主机”选项，添加对方的(运行了冰河服务器端的被攻击主机)IP 地址，如图 4-123 所示。

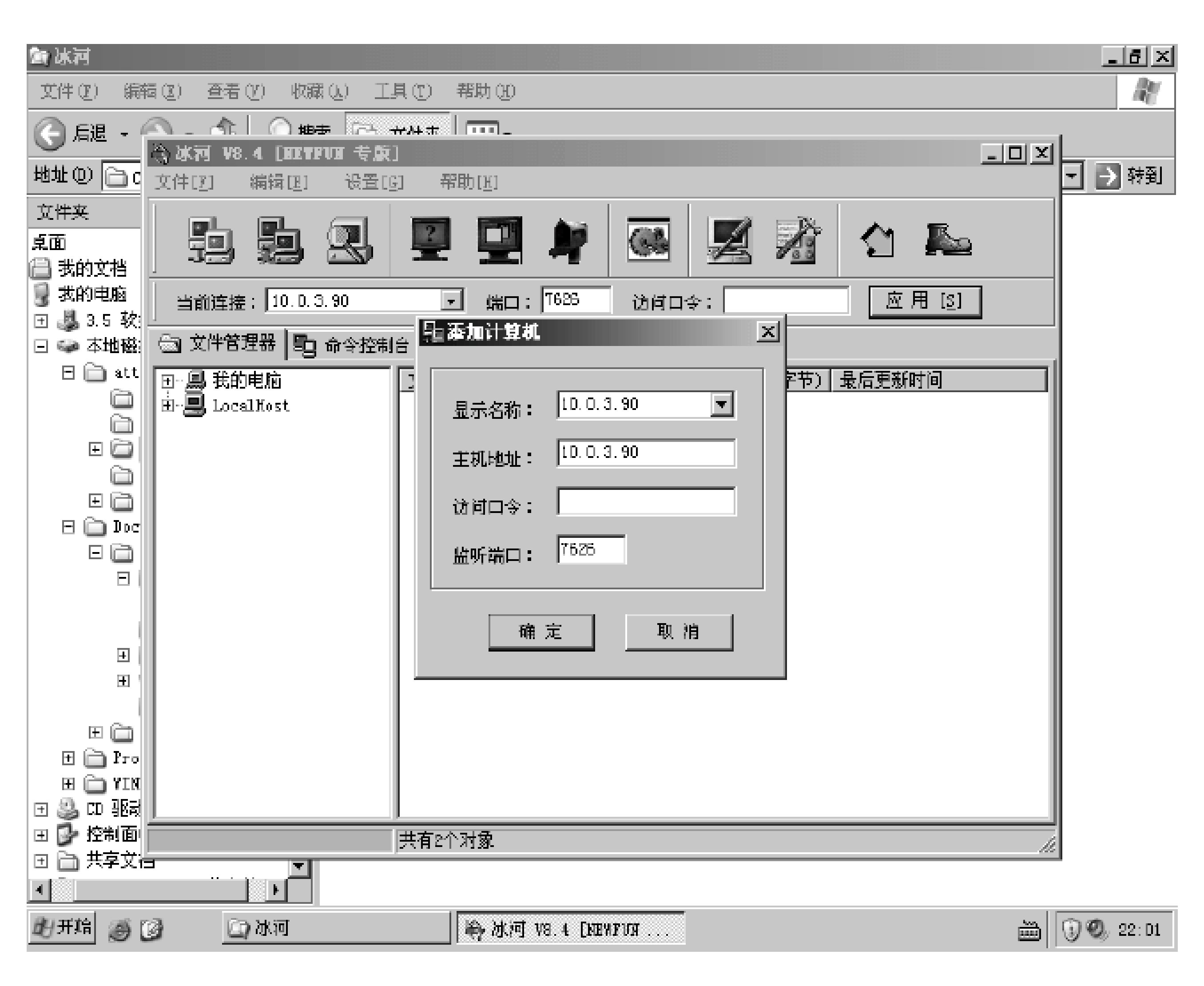



图 4-123　添加对方的 IP 地址

在“文件管理器”列表栏处出现对方主机后双击并进行一系列操作如查看屏幕、文件传输等，如图 4-124 所示。

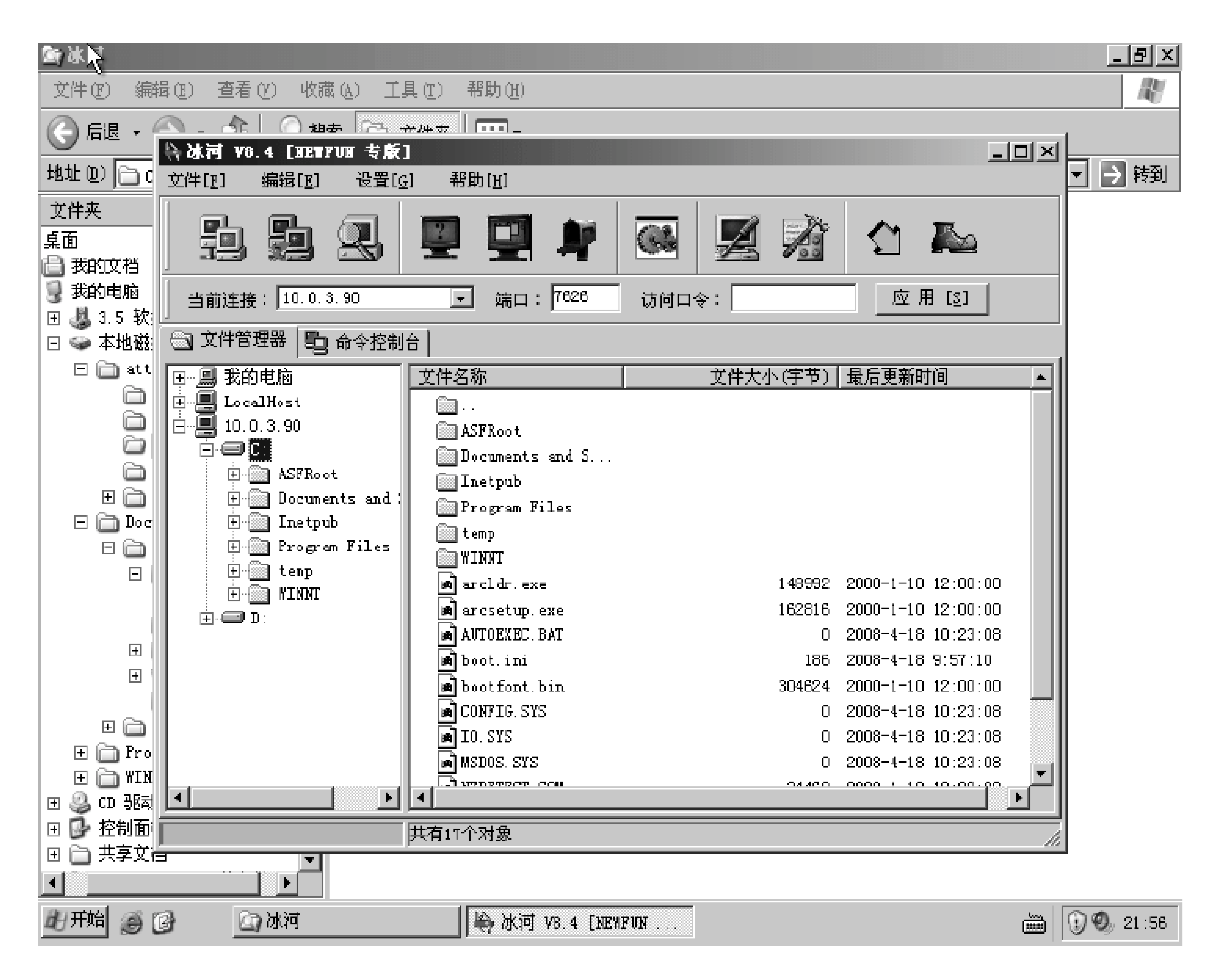



图 4-124　查看对方主机信息

## 3. 查看警报

进入 RG-IDS 控制台，通过“安全事件”组件查看 IDS 检测的安全事件信息，如图 4-125 和图 4-126 所示。




图 4-125　查看 IDS 检测的安全事件信息(1)




图 4-126　查看 IDS 检测的安全事件信息(2)

RG-IDS 将准确检测出 trojans_huigz:huigz_alert 以及 trojans_glactcp:glac_tcp 事件,事件详细信息如图 4-127 和图 4-128 所示。




图 4-127　事件详细信息(1)

## 【注意事项】

本实验中的病毒样本只能用于实验。




图 4-128　事件详细信息(2)

# 4.13　蠕虫病毒传输检测

## 【实验名称】

蠕虫病毒传输检测。

## 【实验目的】

使用 RG-IDS 对蠕虫病毒传输进行检测。

## 【背景描述】

某网络中的 PC 由于使用者的安全意识不强，经常感染蠕虫病毒，导致遭受黑客的攻击和控制。RG-IDS 能及时检测出蠕虫病毒的网络传输行为，并及时上报到控制台。

## 【需求分析】

通过 RG-IDS 实时检测和告警，可以使管理员及时发现并查杀病毒，对遭受攻击的主机进行隔离防御和维护。

## 【实验拓扑】

如图 4-129 所示的网络拓扑，某企业网络管理员发现网络中使用者的安全意识不强，经常遭受黑客的 DDoS 攻击，于是部署了 IDS 系统对 DDoS 攻击进行检测，以实现网络的安全防范功能。

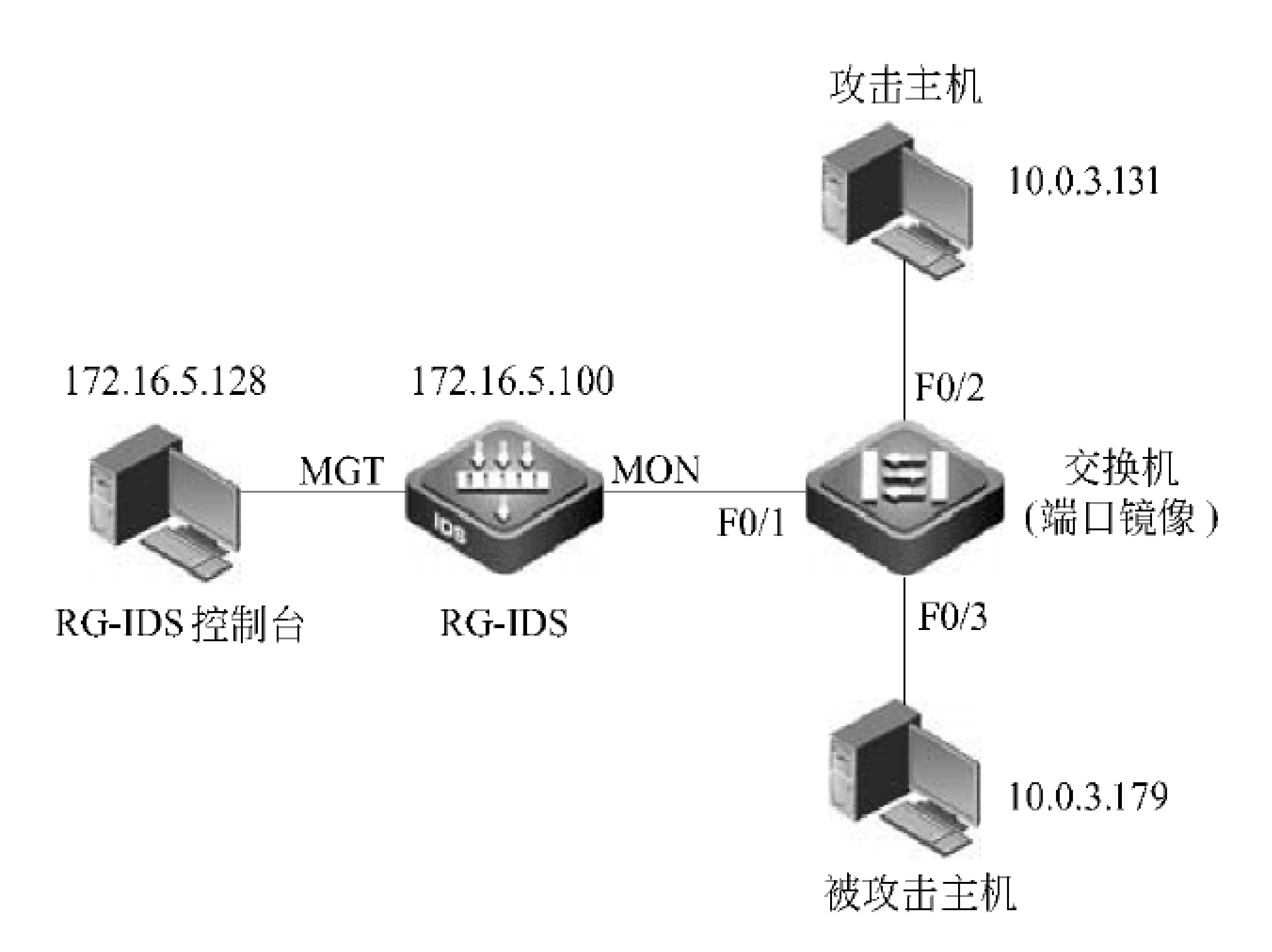



图 4-129　蠕虫病毒传输检测网络拓扑图

## 【实验设备】

| | |
|---|---|
| PC | 3 台 |
| RG-IDS | 1 台 |
| 直连线 | 4 条 |
| 交换机 | 1 台(支持多对一的端口镜像) |
| 攻击软件 | 机器狗和 ANI 蠕虫病毒样本 |
| 攻击主机 | Microsoft Windows 操作系统 |
| 被攻击主机 | IIS 或者 Apache 等 Web 服务器均可 |

## 【预备知识】

- 交换机端口镜像配置。
- RG-IDS 配置。
- 病毒样本。

## 【实验原理】

机器狗本身会释放出一个 pcihdd.sys 文件到 drivers 目录中,pcihdd.sys 是一个底层硬盘驱动,它提高自己的优先级接替还原卡或冰点的硬盘驱动,然后访问指定的网址。这些网址只要连接就会自动下载大量的病毒与恶意插件,然后修改接管启动管理器,还会通过内部网络传播,当一台主机被感染后,能引发整个网络的主机全部自动重启。

ANI 病毒的执行原理和症状:(1)病毒的作者制作恶意 ANI 文件,使其能下载其他的病毒或木马程序;(2)病毒制作者会将 ANI 文件更名为 jpeg、bmp、gif 等常见图片文件放到网页中;(3)当用户利用 IE 浏览器访问这些网页时会自动将该 ANI 文件下载到本地;(4)IE 浏览器在打开该 ANI 文件时,即可触发漏洞,并立即下载和执行其他的病毒或木马程序。

## 【实验步骤】

### 1. 策略编辑

如图 4-130 所示，单击主界面上的“策略”按钮，切换到策略编辑器界面，从现有的策略模板中生成一个新的策略。在新的策略中选择 virus：pgz：pgz_viralbody 以及 virus：anivirosomes：anivirus_viralbody 签名，并将策略下发到引擎中。

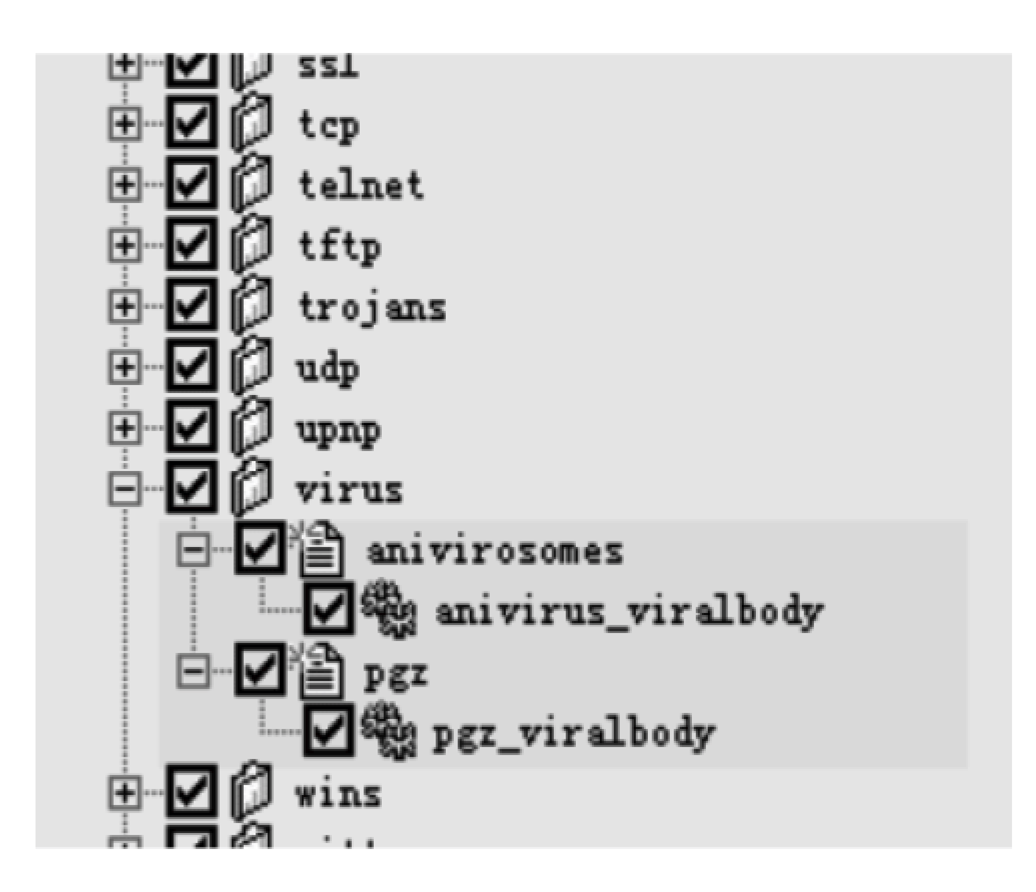



图 4-130　策略编辑器界面

### 2 实施攻击

1）机器狗病毒

将病毒样本和 test. html 文件复制到被攻击主机上，在被攻击主机上开启 IIS 或 Apache 服务，并将 test. html 设为主页。

通过网络中的另外一台主机访问被攻击主机上的 test. html 页面，选择“机器狗测试”，如图 4-131 所示。

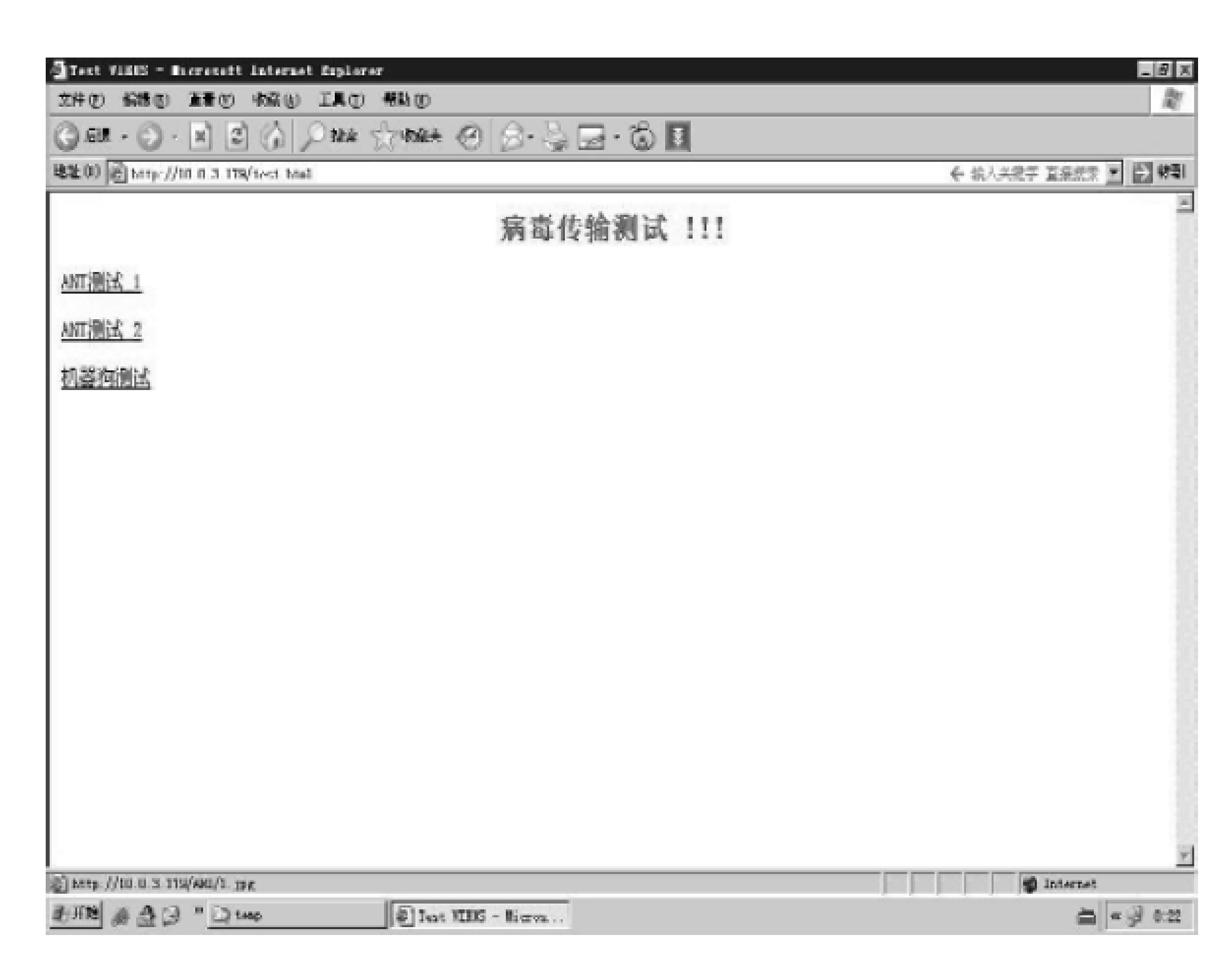



图 4-131　选择“机器狗测试”

按照对话框的提示把 00023.exe 文件下载到本地，如图 4-132 所示。

图 4-132　下载文件

2）ANI 病毒

将病毒样本和 test.html 文件复制到被攻击主机上，在被攻击主机上开启 IIS 或 Apache 服务，并将 test.html 设为主页。

通过网络中的另外一台主机访问被攻击主机上的 test.html 页面，选择“ANI 测试 1”或“ANI 测试 2”，如图 4-133 所示。




图 4-133　选择“ANI 测试 1”或“ANI 测试 2”

在本地打开病毒样本文件。

### 3. 查看警报

进入 RG-IDS 控制台，通过“安全事件”组件查看 IDS 检测的安全事件信息，如图 4-134 和图 4-135 所示。

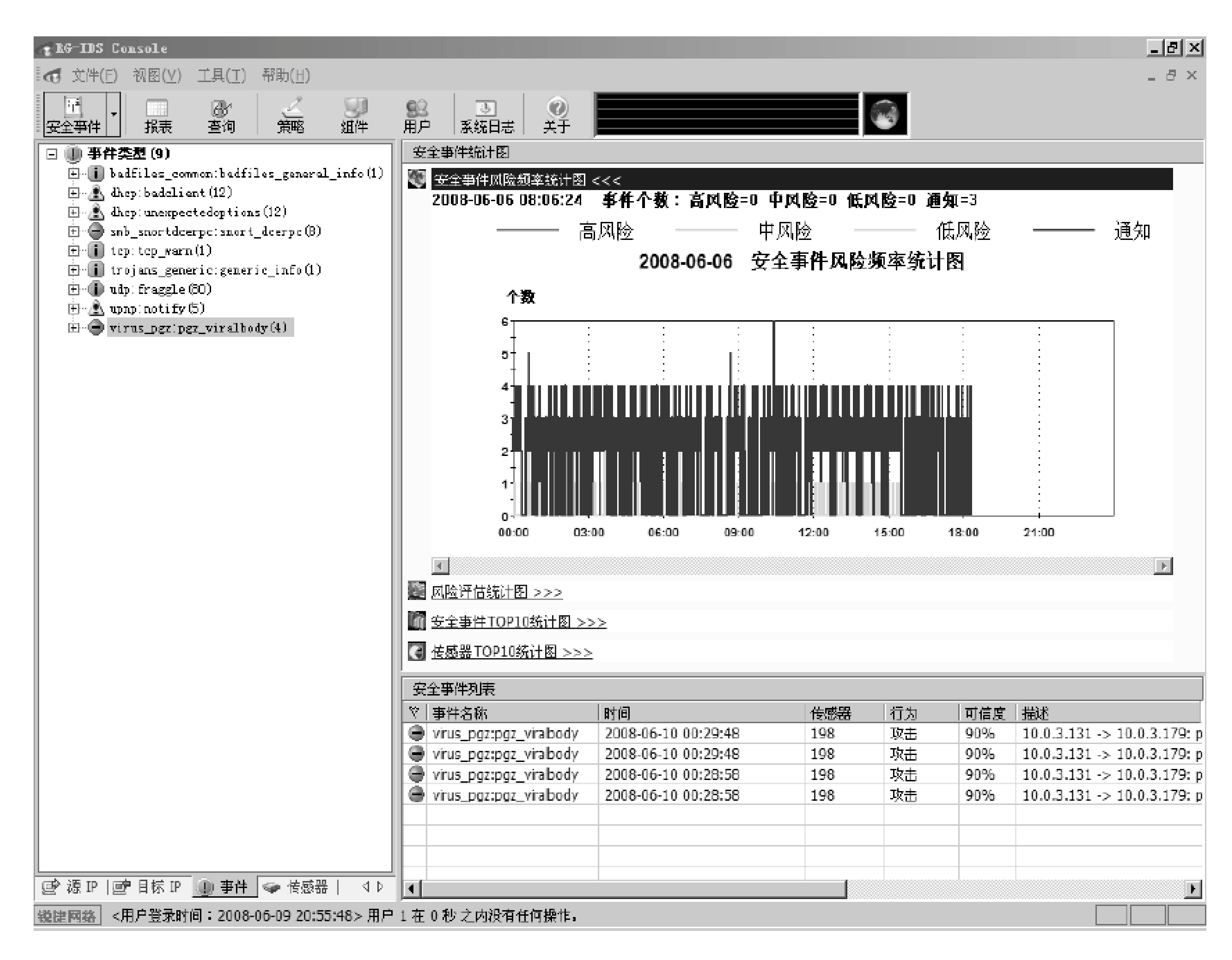



图 4-134　查看 IDS 检测的安全事件信息(1)

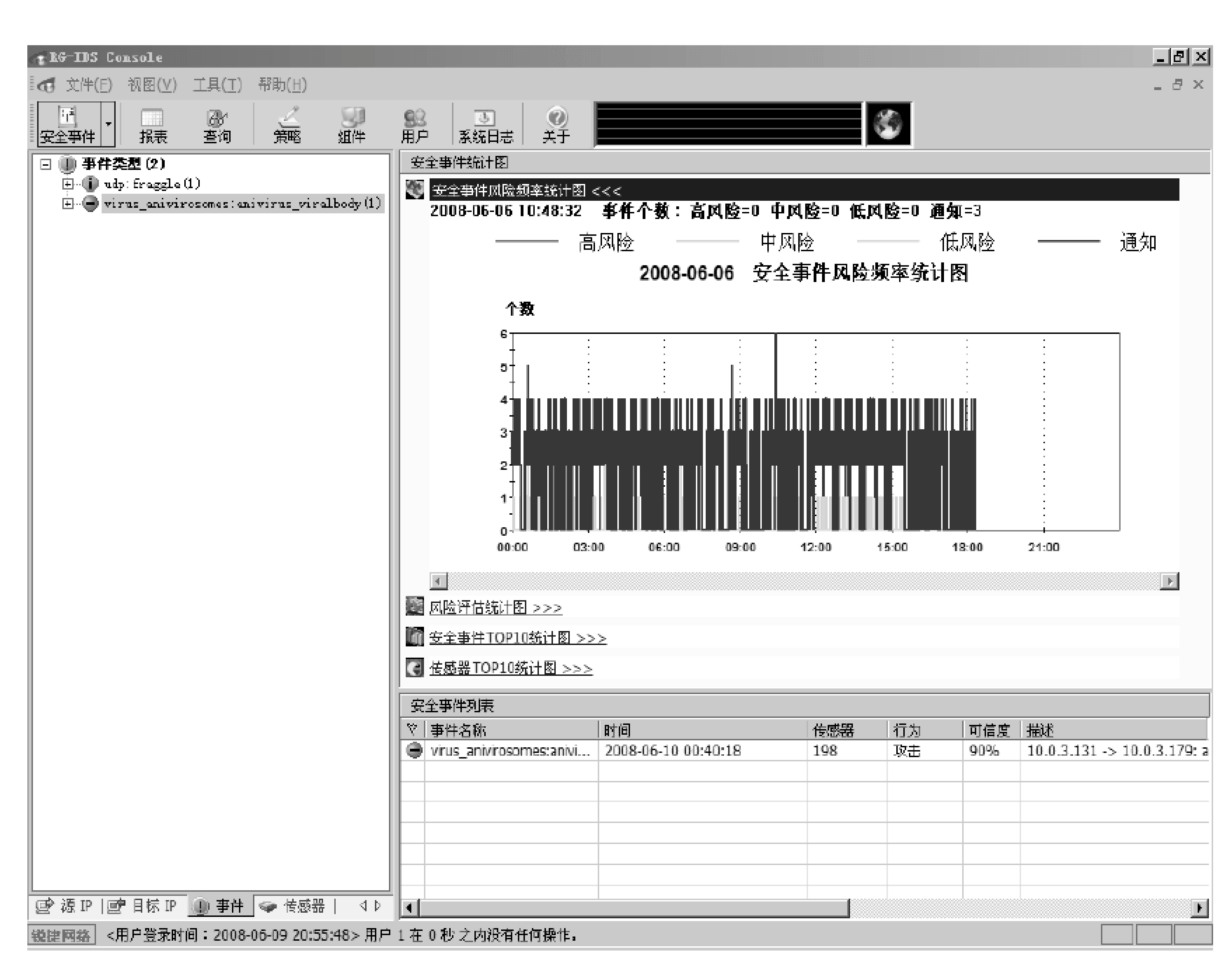



图 4-135　查看 IDS 检测的安全事件信息(2)

RG-IDS 将准确检测出 virus:pgz:pgz_viralbody 以及 virus:anivirosomes:anivirus_viralbody 事件，事件详细信息如图 4-136 和图 4-137 所示。




图 4-136　事件详细信息(1)




图 4-137　事件详细信息(2)

## 【注意事项】

本实验中的病毒样本只能用于实验。

# 4.14 配置 IDS 与防火墙联动

## 【实验名称】

配置 IDS 与防火墙联动。

## 【实验目的】

掌握 RG-IDS 与 RG-WALL 防火墙联动的配置方式，增强对攻击阻断的有效性和及时性。

## 【背景描述】

IDS 产品与防火墙产品联动，能对恶意攻击和流量进行实时检测和防御。

## 【需求分析】

需求：IDS 产品只能单纯地检测不具备防御功能，防火墙只能对 3-4 层数据报文进行处理，不具备深入检测功能。

分析：通过 IDS 检测并将检测信息传递给防火墙，通过防火墙对攻击的地址和端口进行阻断等措施，以达到实时防御的目的。

## 【实验拓扑】

如图 4-138 所示的网络拓扑，某企业网络管理员发现 IDS 产品只能单纯地检测不具备防御功能，防火墙只能对 3-4 层数据报文进行处理，不具备深入检测功能，于是部署了 IDS 与防火墙联动系统，通过 IDS 检测并将检测信息传递给防火墙，通过防火墙对攻击的地址和端口进行阻断等措施，达到防御的目的，以实现网络的安全防范功能。

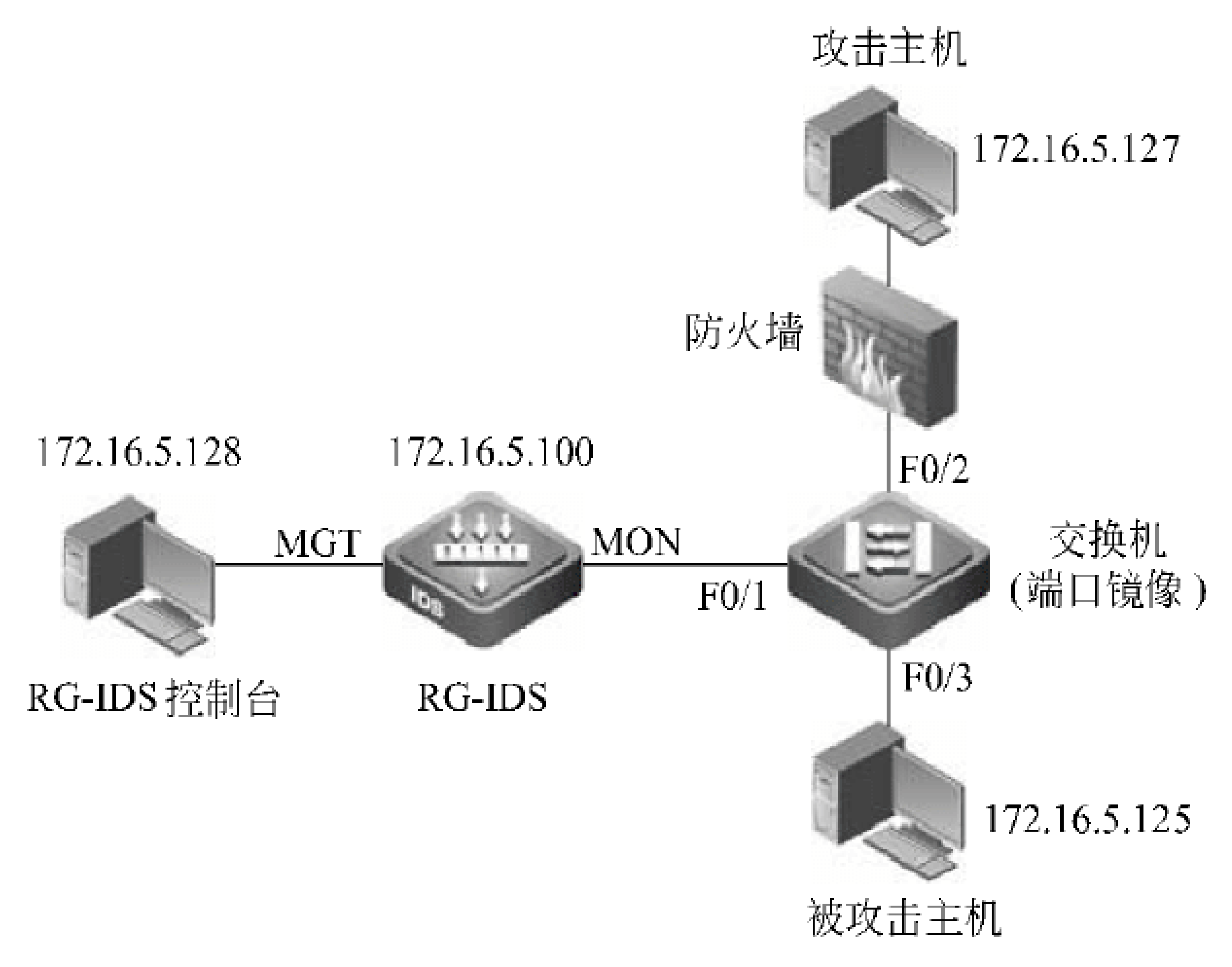



图 4-138　配置 IDS 与防火墙联动网络拓扑图

## 【实验设备】

PC　　　　3 台
防火墙　　1 台
RG-IDS　　1 台
直连线　　若干条
交换机　　1 台(必须支持多对一的端口镜像)
SecureCRT 软件

## 【预备知识】

- RG-WALL 防火墙配置基础。
- 交换机端口镜像配置。
- RG-IDS 配置基础。

## 【实验原理】

入侵检测系统在捕捉到某一攻击事件后,按策略进行检查,如果在策略中对该攻击事件设置了防火墙阻断,那么入侵检测系统就会发给防火墙一个相应的动态阻断策略。防火墙根据该动态策略中的设置进行相应的阻断,阻断的时间、阻断时间间隔、源端口、目的端口、源 IP 和目的 IP 等信息,完全依照入侵检测系统发出的动态策略来执行。

在本实验中,以 Ping-of-Death 签名为攻击事件,在没有配置为联动的响应方式之前,攻击主机能够向被攻击主机发送超大字节的 ICMP 报文,并被 IDS 检测到。实施 RG-IDS 与 RG-WALL 联动后,IDS 首先检测到 Ping-of-Death 攻击,并将事件的信息包括源、目的地址等通过 SSH 通知防火墙,防火墙根据 IDS 发送的攻击事件信息自动生成响应规则,阻断攻击源和目的之间的通信。

## 【实验步骤】

### 1. 配置策略

如图 4-139 所示,单击主界面上的“策略”按钮,切换到策略编辑器界面,从现有的策略模板中生成一个新的策略。在新的策略中选择 pingofdeath 签名,并将策略并下发到引擎中。

### 2 超大字节 ICMP 报文攻击测试

攻击主机 172.16.5.127 向目标主机 172.16.5.125 发送超大字节 ICMP 报文,如图 4-140 所示。

通过 RG-IDS 控制台“安全事件”组件查看 IDS 检测的安全事件信息,pingofdeath 事件上报数量约为 200 条,如图 4-141 所示。

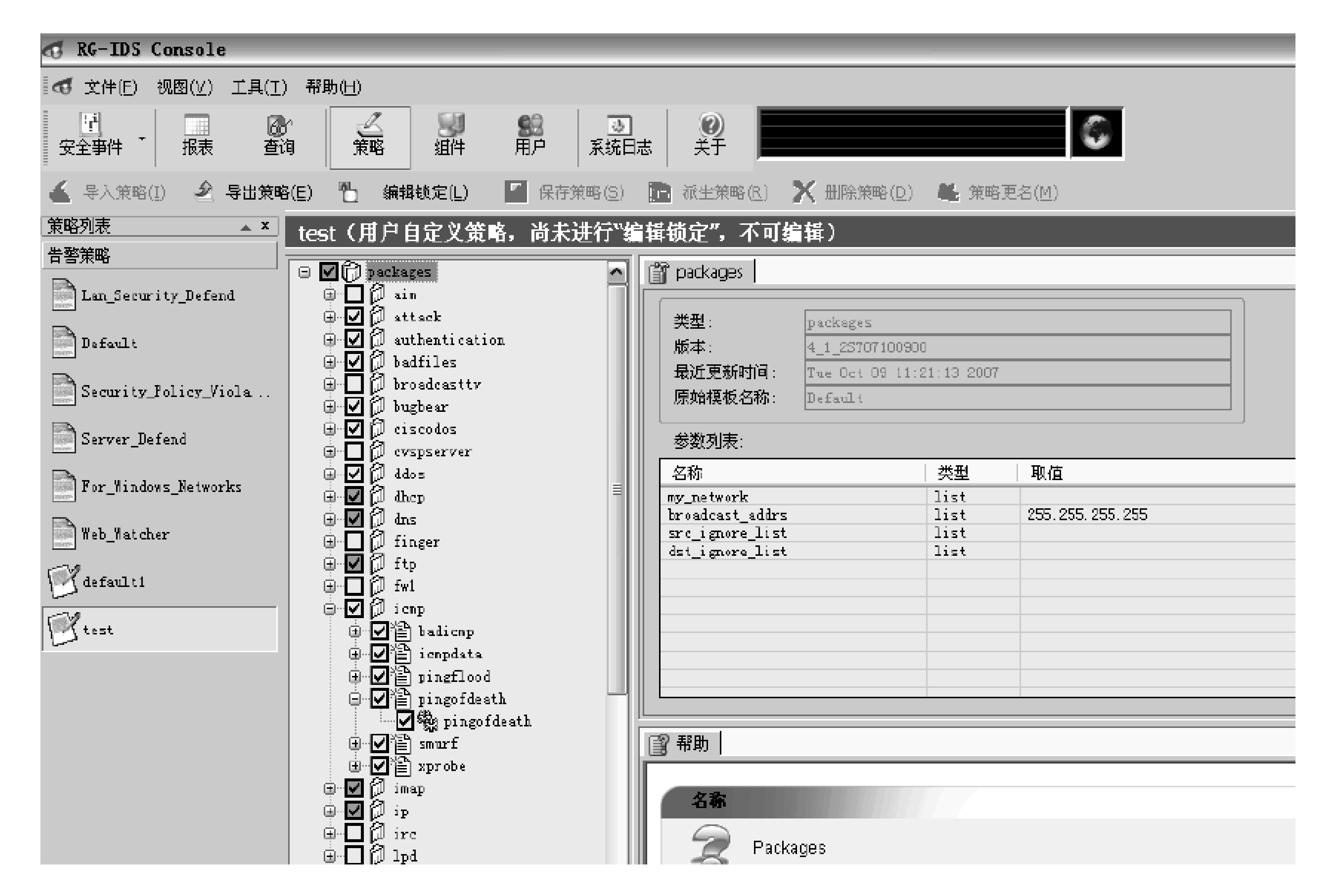



图 4-139　IDS 策略编辑器界面

```
C:\Documents and Settings\Administrator>ping 172.16.5.125 -l 65000

Pinging 172.16.5.125 with 65000 bytes of data:

Reply from 172.16.5.125: bytes=65000 time=13ms TTL=128
Reply from 172.16.5.125: bytes=65000 time=11ms TTL=128
Reply from 172.16.5.125: bytes=65000 time=11ms TTL=128
Reply from 172.16.5.125: bytes=65000 time=11ms TTL=128

Ping statistics for 172.16.5.125:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 11ms, Maximum = 13ms, Average = 11ms
```

图 4-140　超大字节 ICMP 报文攻击测试

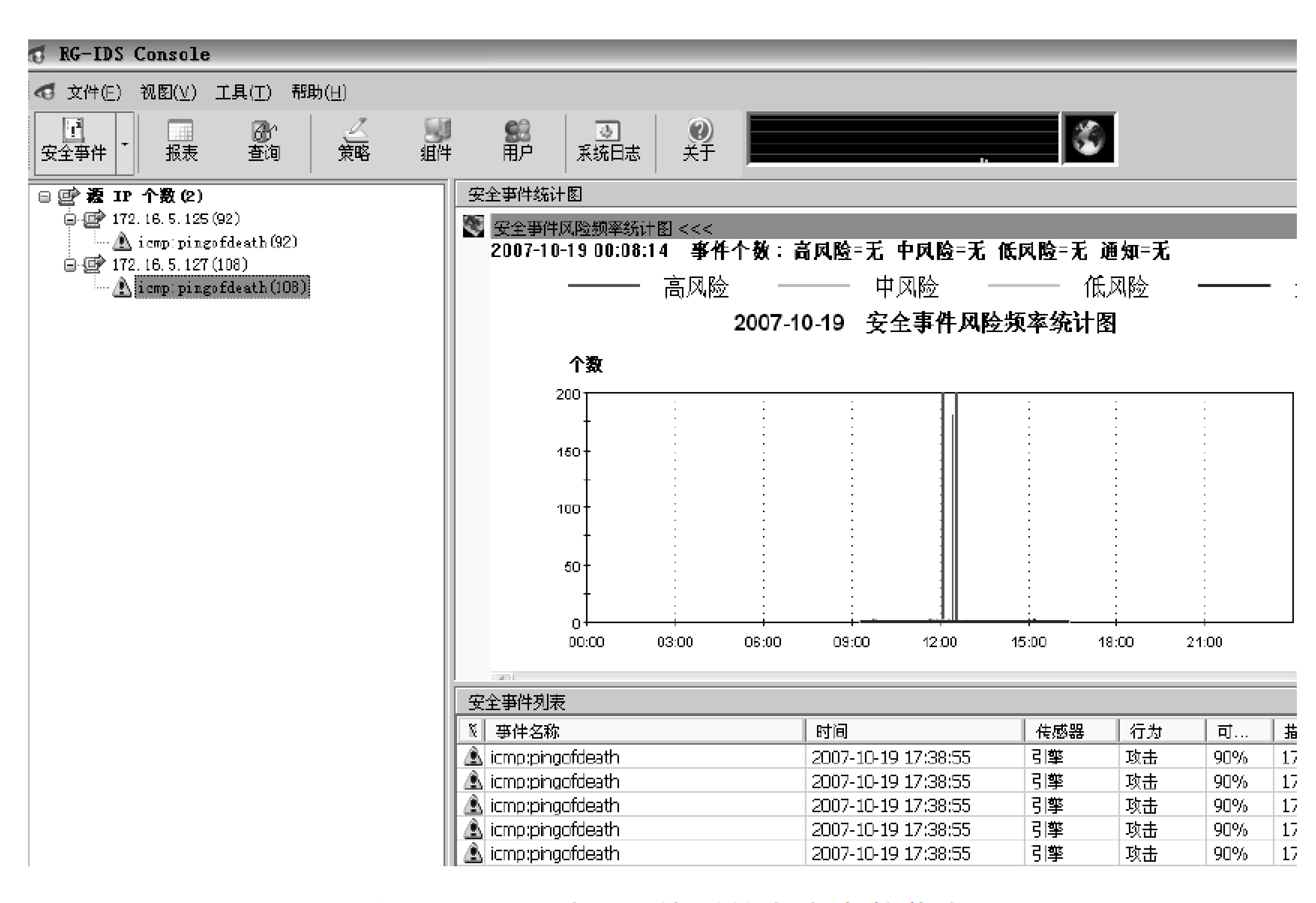



图 4-141　查看 IDS 检测的安全事件信息

### 3. RG-IDS 联动文件修改

将 ECRunning. cfg 和 scrtcmd. vbs 两个文件复制到事件收集器的安装目录下覆盖原有文件，如图 4-142 所示。




图 4-142　RG-IDS 联动文件修改

ECRunning. cfg 和 scrtcmd. vbs 两个文件需要单独获取。

### 4. 配置响应参数

在 RG-IDS 控制台的“策略”配置界面，选择“响应参数配置”区域中的 Global_Settings 文件，在“请输入响应应用程序的名称”文本框中输入 ruijie，如图 4-143 所示。




图 4-143　配置响应参数

单击 保存策略(S) 按钮，保存修改。

### 5. 配置联动签名的响应方式

进入策略配置界面，选择需要联动的签名 pingofdeath，并在右侧响应方式中选择 DISPLAY、LOGDB 和 USER，为攻击签名选择响应方式，如图 4-144 所示。

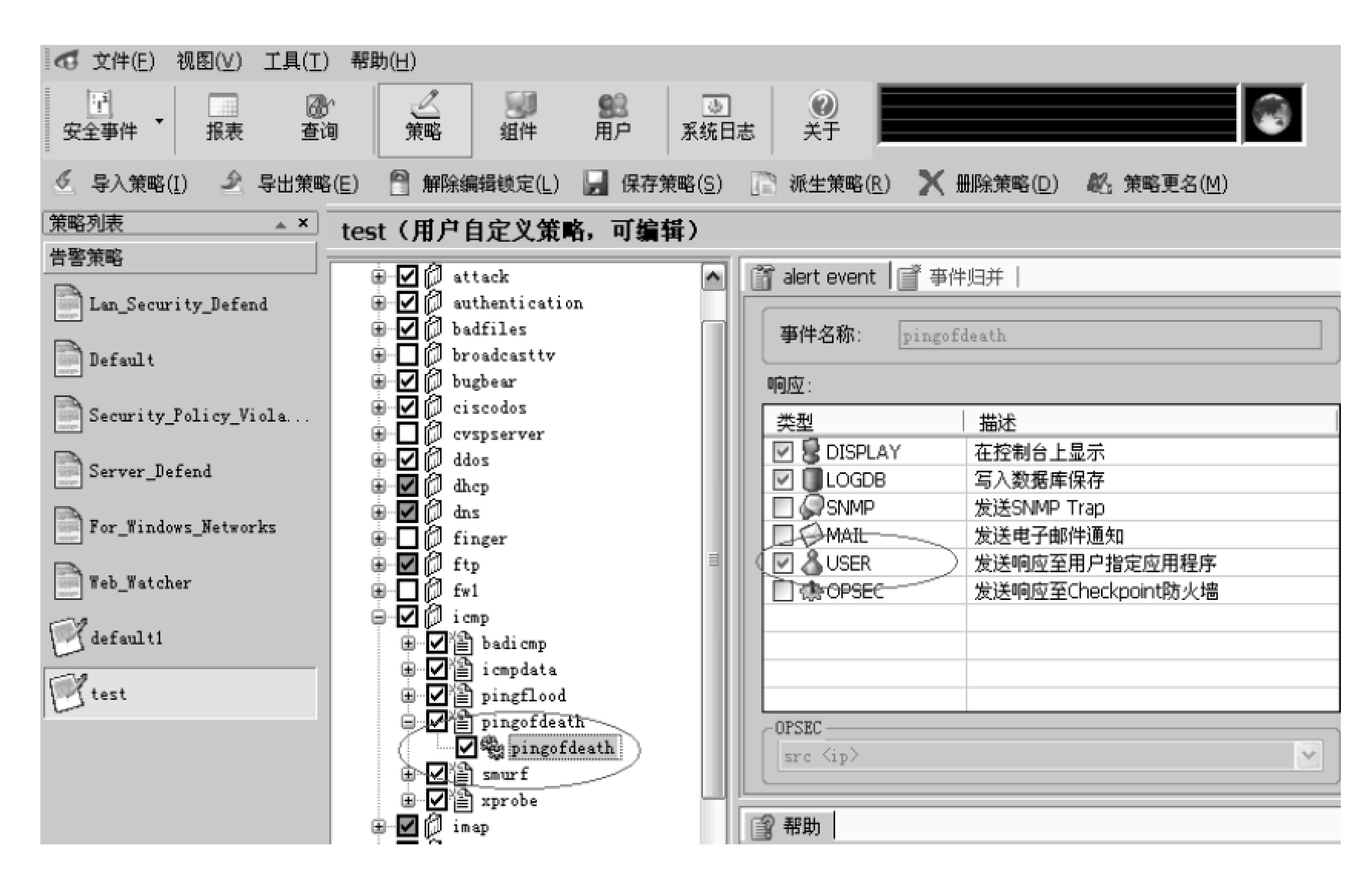


图 4-144　配置联动签名的响应方式

单击 保存策略(S) 按钮，保存修改。

通过 RG-IDS 应用服务管理器，重新启动“事件收集服务”、“安全事件响应服务”和“IDS 数据管理服务”，如图 4-145 所示。



图 4-145　启动事件收集服务

### 6. 建立防火墙 SSH 连接

在 IDS 控制台 PC 上，使用 SecureCRT 工具，建立名为 ruijie 的 SSH 连接，使用该连接可以通过 SSH 登录 RG-WALL 防火墙，如图 4-146 所示。

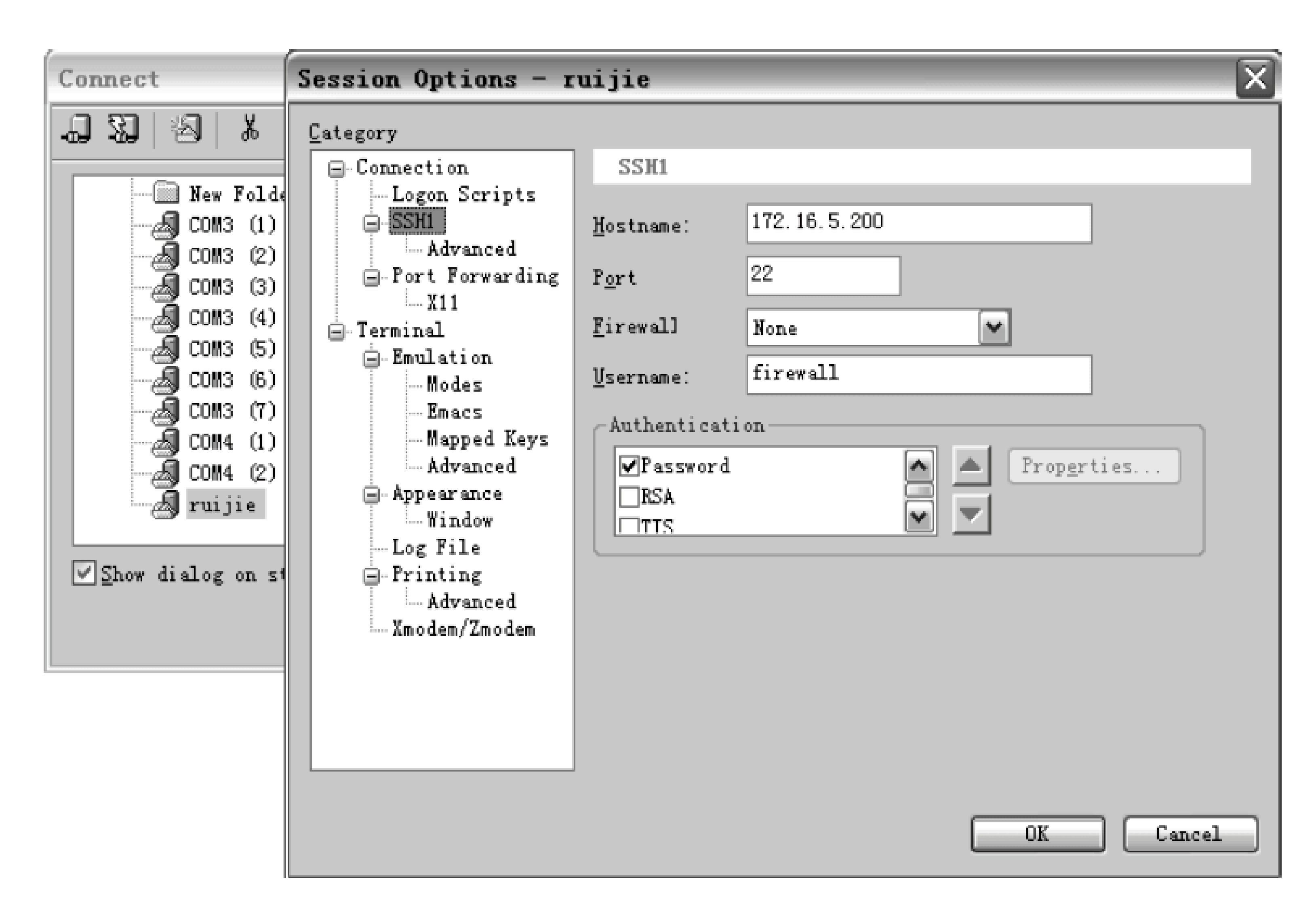



图 4-146　建立防火墙 SSH 连接

通过 SSH 连接登录防火墙一次，登录过程中要选择保存证书、用户名和密码等信息，登录成功后退出该程序。

### 7. ICMP 攻击

攻击主机 172.16.5.127 向目标主机 172.16.5.125 发送超大字节 ICMP 报文，如图 4-147 所示。

```
C:\Documents and Settings\Administrator>ping 172.16.5.125 -l 65000

Pinging 172.16.5.125 with 65000 bytes of data:

Reply from 172.16.5.125: bytes=65000 time=13ms TTL=128
Reply from 172.16.5.125: bytes=65000 time=11ms TTL=128
Reply from 172.16.5.125: bytes=65000 time=11ms TTL=128
Reply from 172.16.5.125: bytes=65000 time=11ms TTL=128

Ping statistics for 172.16.5.125:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 11ms, Maximum = 13ms, Average = 11ms
```

图 4-147　ICMP 攻击

通过 RG-IDS 控制台“安全事件”组件查看 IDS 检测的安全事件信息，pingofdeath 事件上报数量约为 200 条，如图 4-148 所示。

### 8. 发送 ICMP 攻击报文

攻击主机 172.16.5.127 发送 ICMP 报文失败，如图 4-149 所示。

### 9. 查看防火墙状态

查看防火墙规则表，防火墙写入规则阻断了攻击主机 172.16.5.127 到目标主机 172.16.5.125 的所有通信，如图 4-150 所示。

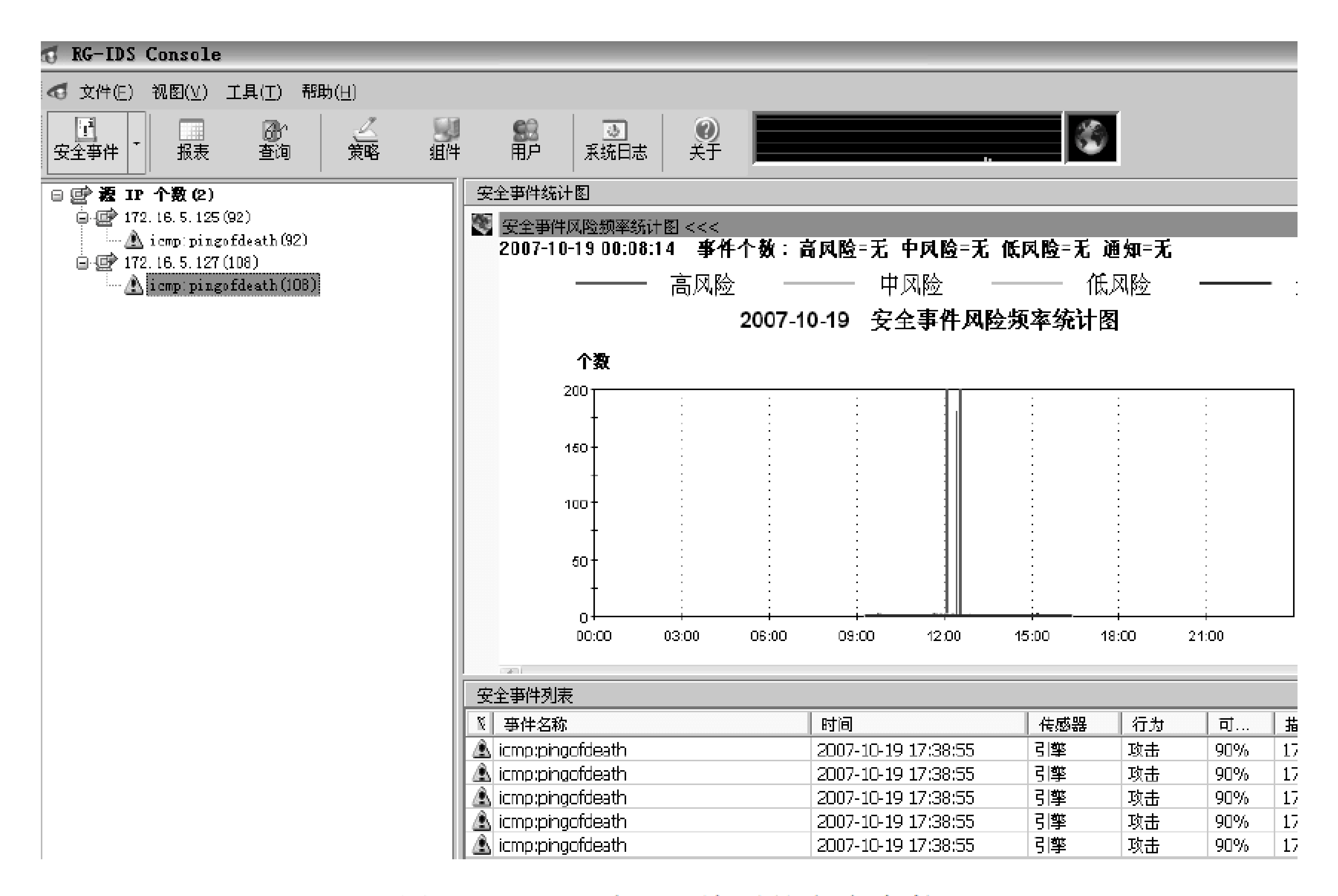



图 4-148　查看 IDS 检测的安全事件

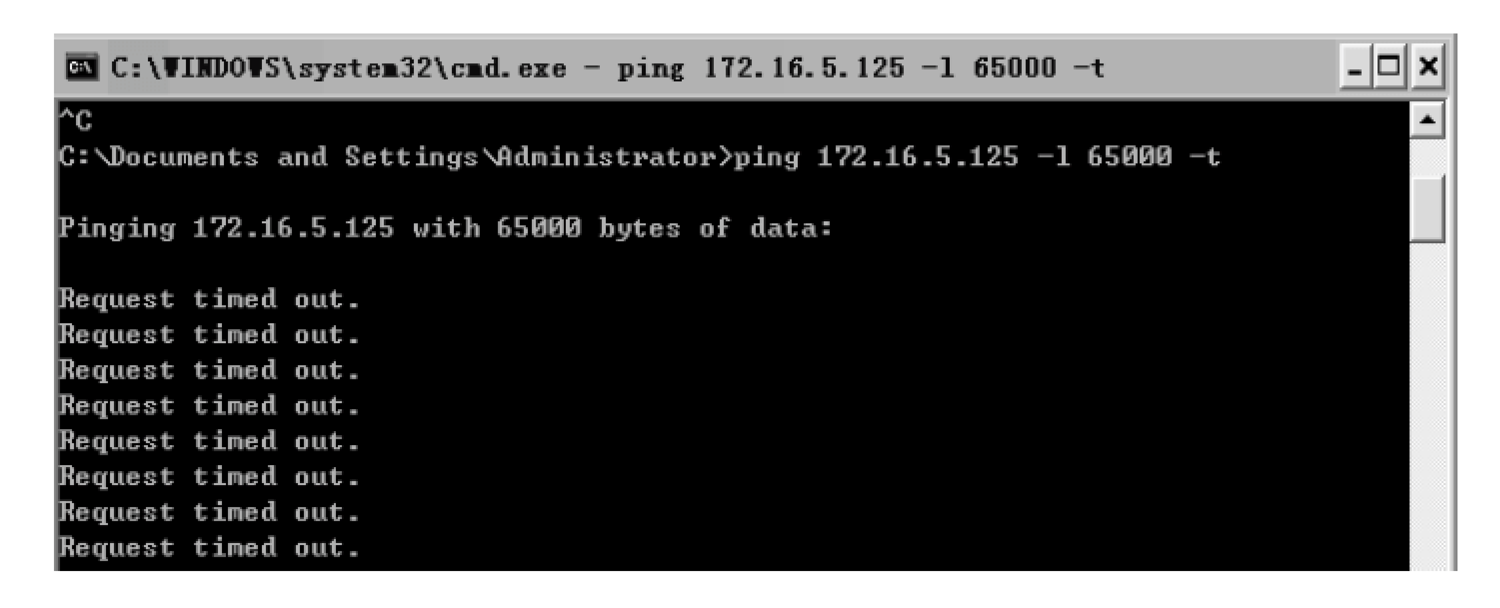
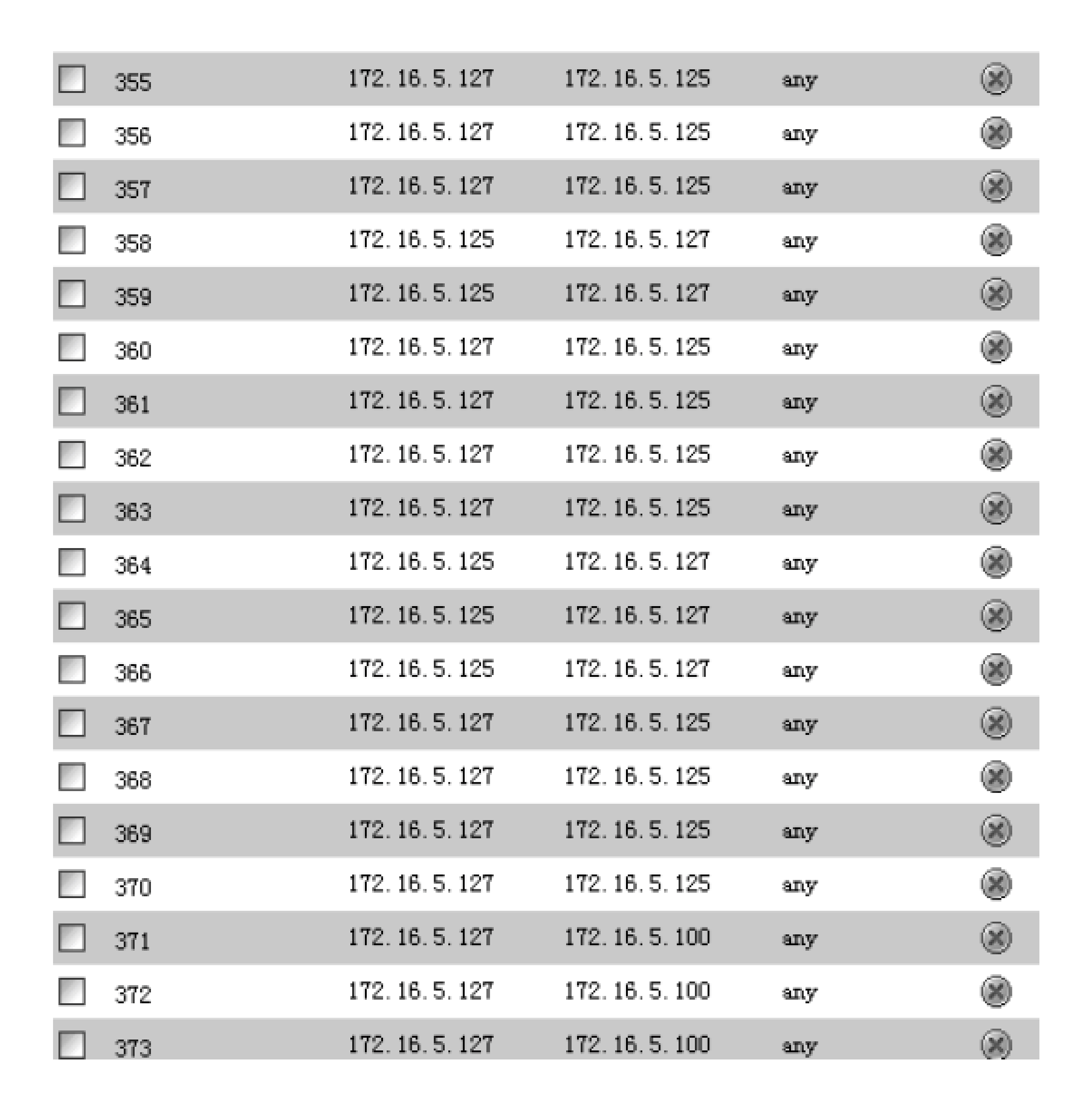



图 4-149　攻击主机发送 ICMP 报文失败



| | | | |
|---|---|---|---|
| 355 | 172.16.5.127 | 172.16.5.125 | any |
| 356 | 172.16.5.127 | 172.16.5.125 | any |
| 357 | 172.16.5.127 | 172.16.5.125 | any |
| 358 | 172.16.5.125 | 172.16.5.127 | any |
| 359 | 172.16.5.125 | 172.16.5.127 | any |
| 360 | 172.16.5.127 | 172.16.5.125 | any |
| 361 | 172.16.5.127 | 172.16.5.125 | any |
| 362 | 172.16.5.127 | 172.16.5.125 | any |
| 363 | 172.16.5.127 | 172.16.5.125 | any |
| 364 | 172.16.5.125 | 172.16.5.127 | any |
| 365 | 172.16.5.125 | 172.16.5.127 | any |
| 366 | 172.16.5.125 | 172.16.5.127 | any |
| 367 | 172.16.5.127 | 172.16.5.125 | any |
| 368 | 172.16.5.127 | 172.16.5.125 | any |
| 369 | 172.16.5.127 | 172.16.5.125 | any |
| 370 | 172.16.5.127 | 172.16.5.125 | any |
| 371 | 172.16.5.127 | 172.16.5.100 | any |
| 372 | 172.16.5.127 | 172.16.5.100 | any |
| 373 | 172.16.5.127 | 172.16.5.100 | any |

图 4-150　查看防火墙状态

### 10. 验证测试

用攻击主机 172.16.5.27 连接被攻击主机 172.16.5.125，返回信息连接失败，如图 4-151 所示。

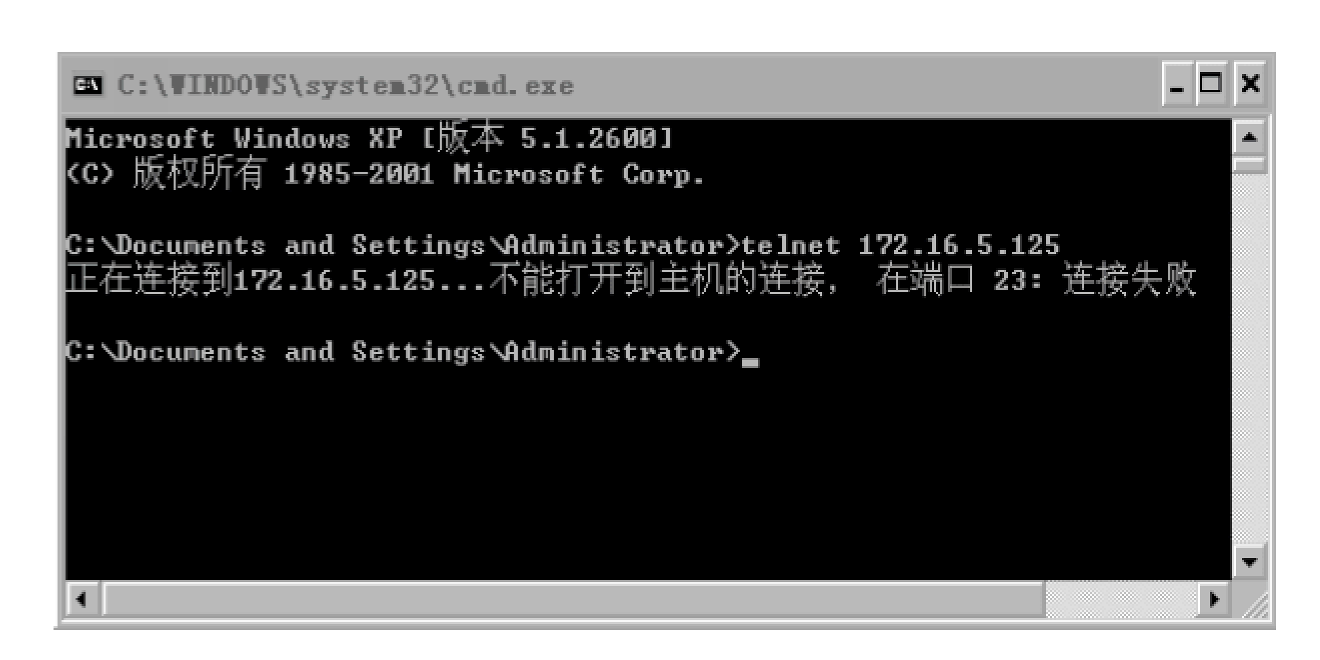



图 4-151 验证测试信息

证明攻击主机 172.16.5.27 到被攻击主机 172.16.5.125 所有通信被阻断，RG-IDS 与 RG-WALL 防火墙联动成功。

## 【注意事项】

- 在实施联动之前，必须通过 SSH 先连接防火墙，并保存证书、账户和密码。
- 在实验过程中，请注意及时清理安全事件列表中的事件信息。
- 防火墙不具备动态规则功能，因此，当事件量比较大时会产生非常多的访问规则，这些规则只能手工删除，过多的规则会严重影响防火墙的性能。
- 本实验没有给出 RG-WALL 防火墙的基本配置，关于 RG-WALL 防火墙的配置，请参见相关的实验和配置文档。

# 4.15 使用自定义事件进行检测

## 【实验名称】

使用自定义事件进行检测。

## 【实验目的】

根据网络的实际情况自定义告警事件。

## 【背景描述】

RG-IDS 出厂时的签名库可能不满足检测需求，所以管理员希望根据网络中的实际情况进行特定的检测。

## 【需求分析】

管理员有针对性地把某些受关注的安全事件添加到特殊事件列表中，从而大大提高工作效率。RG-IDS 出厂时都对事件检测参数提供了一套推荐的方案，但每个网络环境实际情况都不一样，管理员对某些事件的参数进行相应的修改、优化，可使 RG-IDS 更准确地告警。

## 【实验拓扑】

如图 4-152 所示的网络拓扑，某企业网络管理员发现网络中使用 RG-IDS 出厂时的签名库可能不满足检测需求，管理员希望根据网络中的实际情况进行特定的检测，于是部署了 IDS 系统，对网络环境实际情况某些事件的参数进行相应的修改、优化，可使 RG-IDS 更准确地告警，以实现网络的安全防范功能。

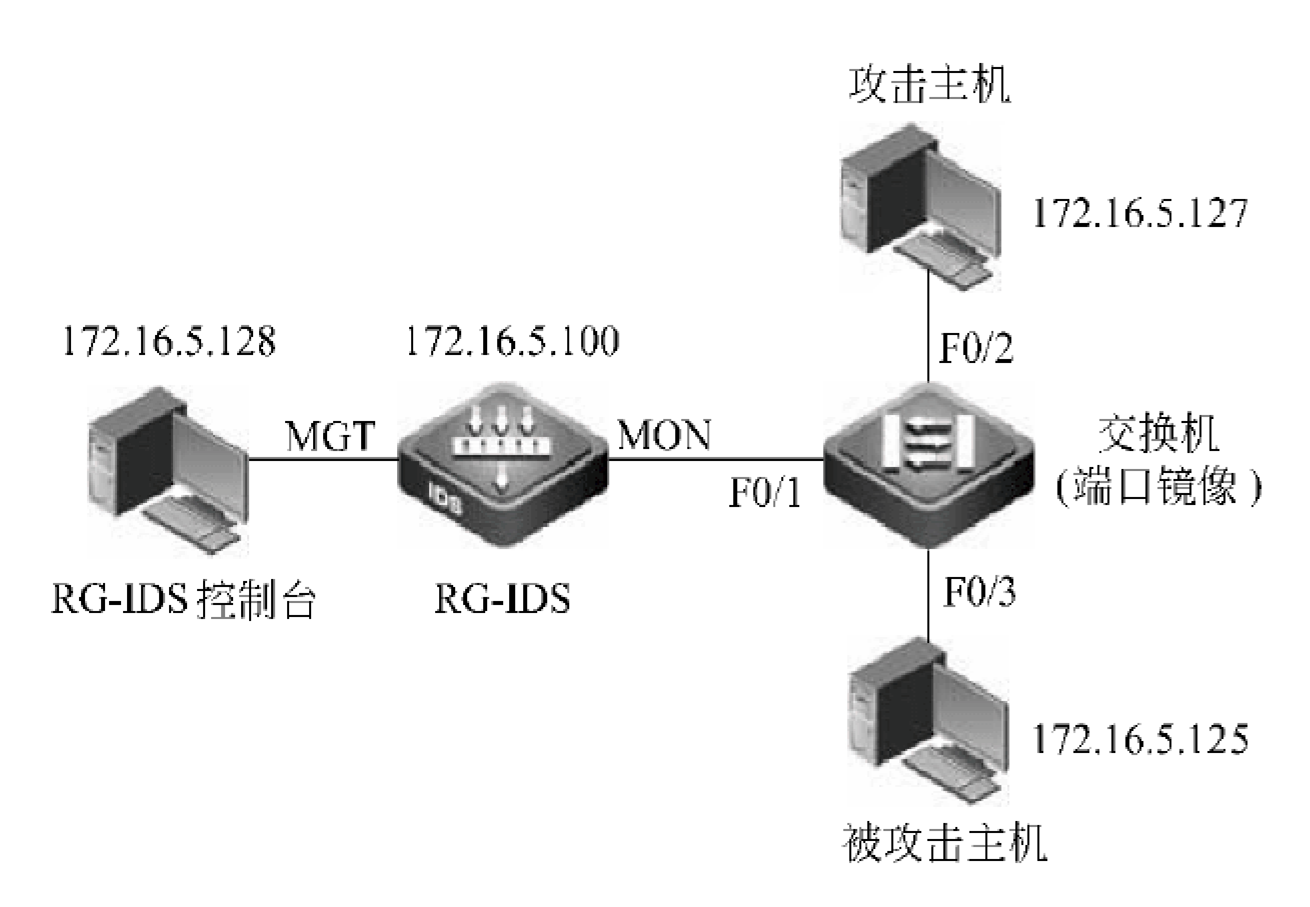



图 4-152　自定义 IDS 事件进行检测网络拓扑图

## 【实验设备】

| | |
|---|---|
| PC | 3 台 |
| RG-IDS Sensor | 1 台 |
| 直连线 | 4 条 |
| 交换机 | 1 台(支持多对一的端口镜像) |

## 【预备知识】

RG-IDS 配置。

## 【实验原理】

事件列表窗口类似于告警策略列表窗口，其中显示用户(策略管理员)定义的特殊事件组。策略管理员从一般事件攻击签名中选择对用户监控更有意义的特殊事件，再将攻

击签名插入到特殊事件组中。具有事件查看权限的安全事件查看员可以查看特殊事件列表。

## 【实验步骤】

### 1. 特殊事件应用

1）添加特殊事件签名

如图 4-153 所示，进入告警策略窗口，展开“一般事件树”，右键单击某个攻击签名，在弹出的菜单中选择“添加到特殊事件窗口”命令。

在弹出的对话框中输入新建事件组的名称，如图 4-154 所示。

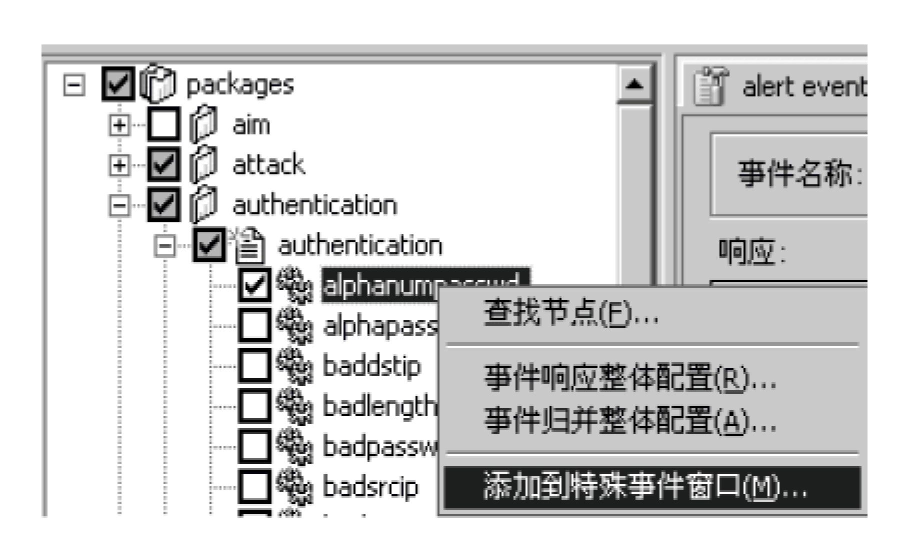



图 4-153　添加特殊事件签名

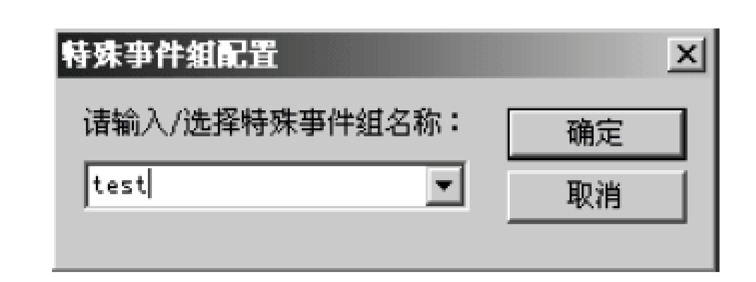



图 4-154　输入新建事件组的名称

单击“确定”按钮，该攻击签名将出现在特殊事件窗口中。

2）特殊事件统计配置

进入告警策略窗口，右键单击“特殊事件树”的树根节点(也可以选中某个 Backend 或者 Package 节点配置，这样响应只针对该节点下面的子节点生效)，如图 4-155 所示。

在弹出的菜单中选择“事件统计整体配置”命令，在弹出的对话框中设置统计条件，如图 4-156 所示。

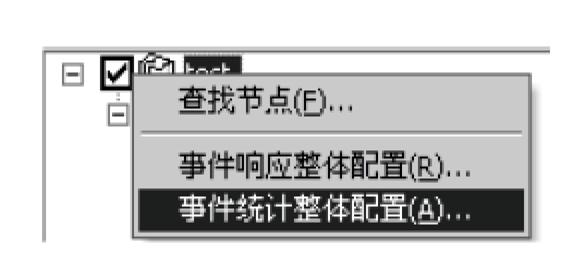



图 4-155　特殊事件统计配置

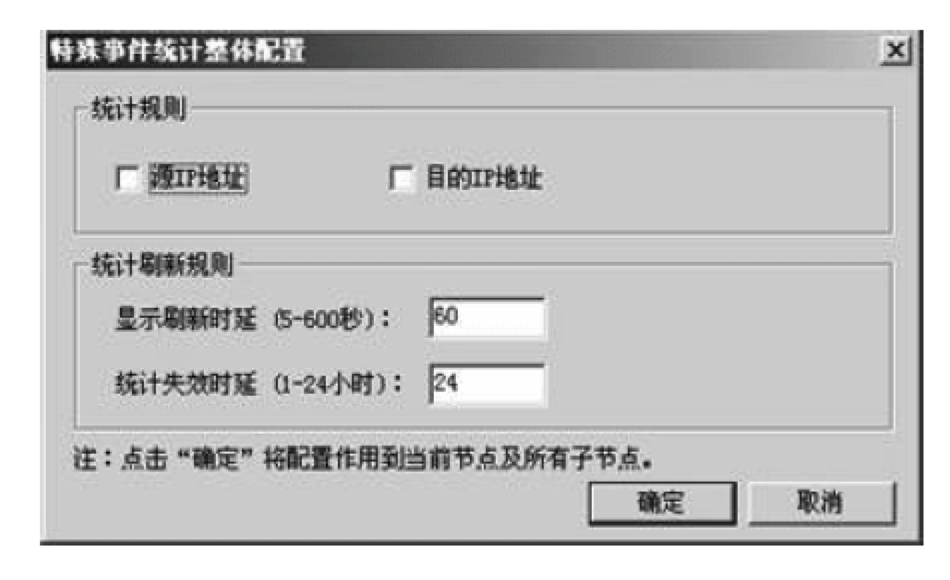



图 4-156　设置统计条件

单击“确定”按钮，特殊事件统计整体配置就完成了。

3）特殊事件查看

特殊事件统计配置完成后，当收到特殊事件后，就可以进入“特殊安全事件统计列表”中查看统计事件。

在“事件”窗口中单击工具栏上的“特殊事件统计”按钮。事件详细列表窗口由 3 部分组成，即“特殊事件列表”、“特殊事件统计”和“帮助”，如图 4-157 所示。

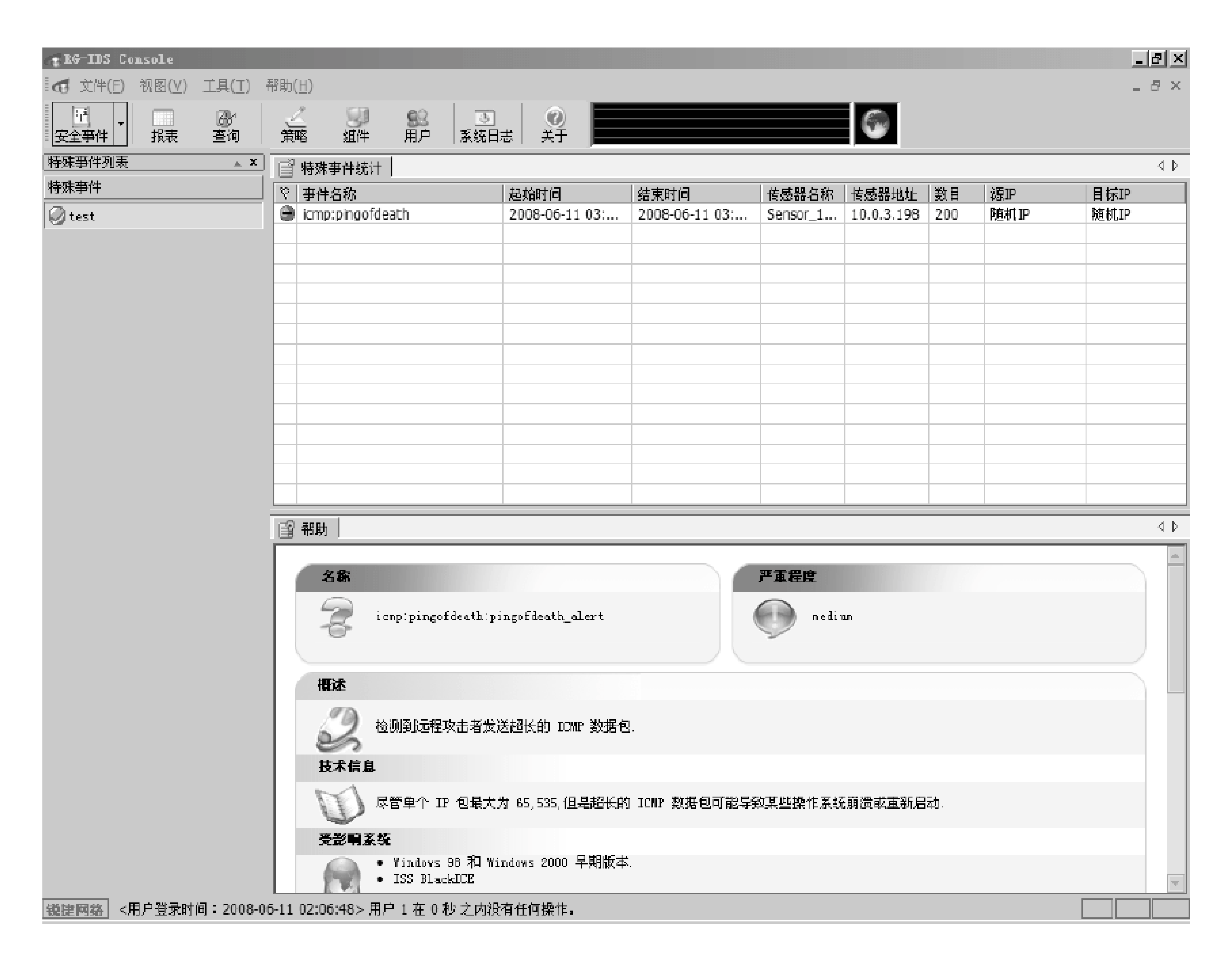



图 4-157　查看特殊事件

## 2 事件参数的配置

1）事件背景

某局域网内架设了一台 FTP 服务器，该服务器用户名为 rjids，密码为 2008，由于该密码安全性低易被猜解，管理员希望能在 IDS 事件告警中体现出来。

2）用户登录 FTP

该用户登录 FTP，在默认情形下 RG-IDS 无告警，如图 4-158 和图 4-159 所示。




图 4-158　用户登录 FTP

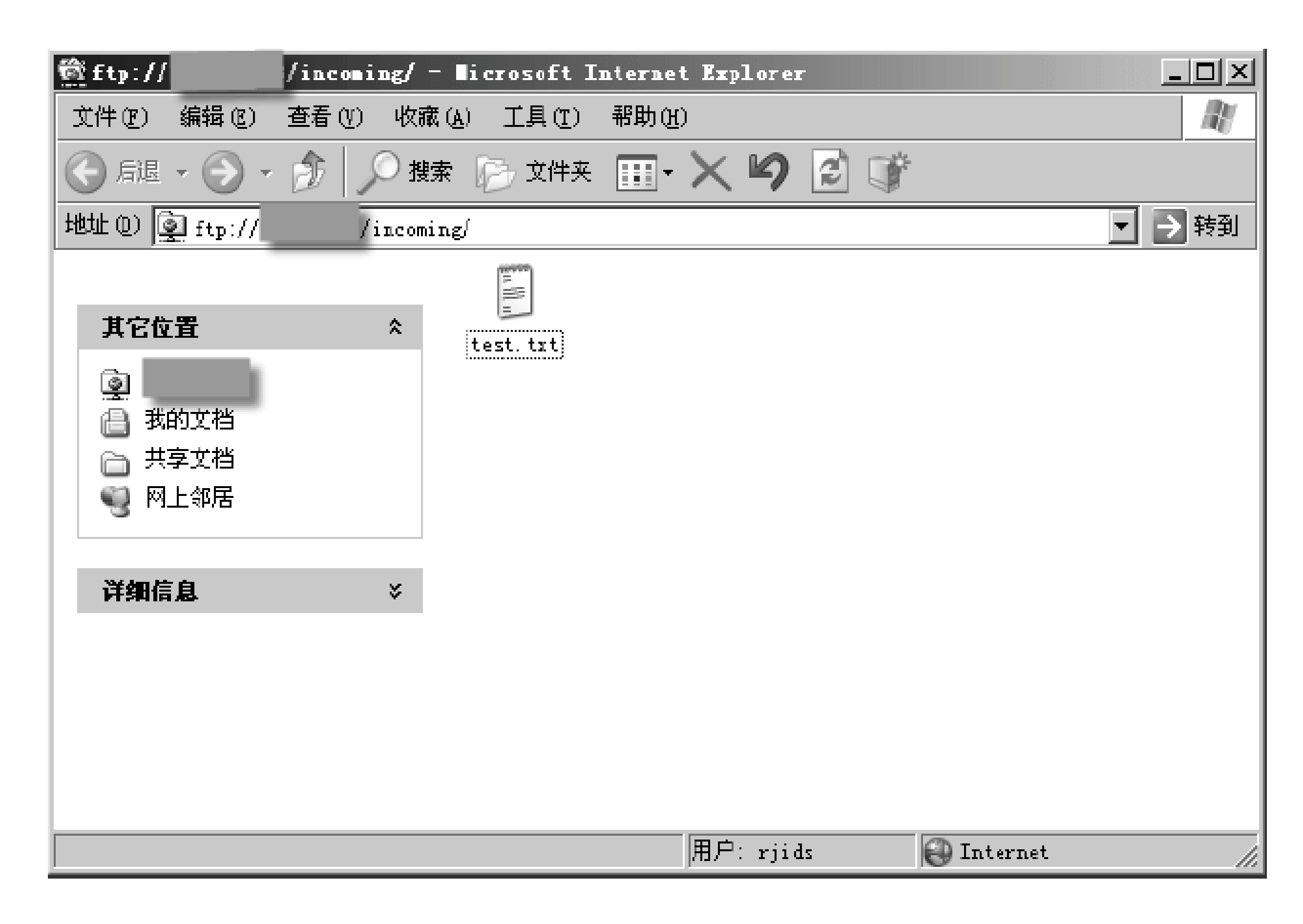



图 4-159　用户登录 FTP 默认情形下 RG-IDS 无告警

3）修改事件参数

单击 策略 按钮，找到正在使用的策略下的 authentication：authentication 节点，如图 4-160 所示。

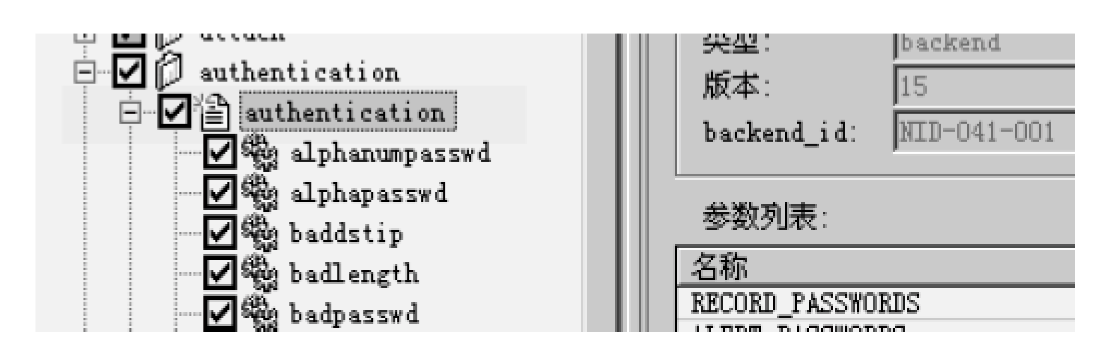



图 4-160　修改事件参数(1)

单击 编辑锁定(L) 按钮，对 authentication：authentication 下的 BAD_PASSWORD_LIST 参数进行修改，如图 4-161 所示。

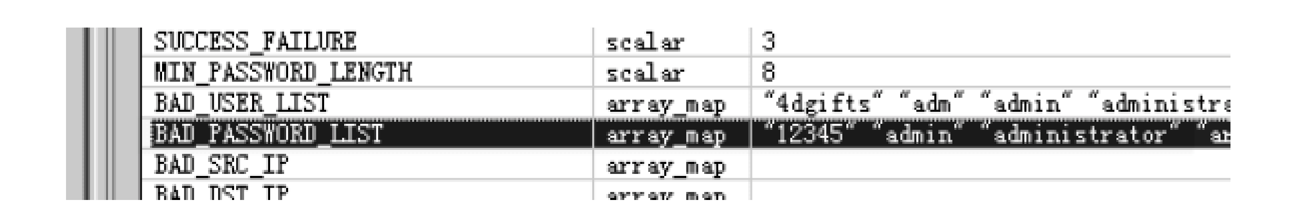



图 4-161　修改事件参数(2)

把不安全的密码“2008”(注意必须把两端的引号也添加上)添加到列表中，如图 4-162 所示。




图 4-162　添加不安全的密码

单击“确定”按钮，保存并重新应用策略。

4）验证事件参数修改

再次使用该账号、密码登录 FTP，RG-IDS 产生告警，如图 4-163 和图 4-164 所示。

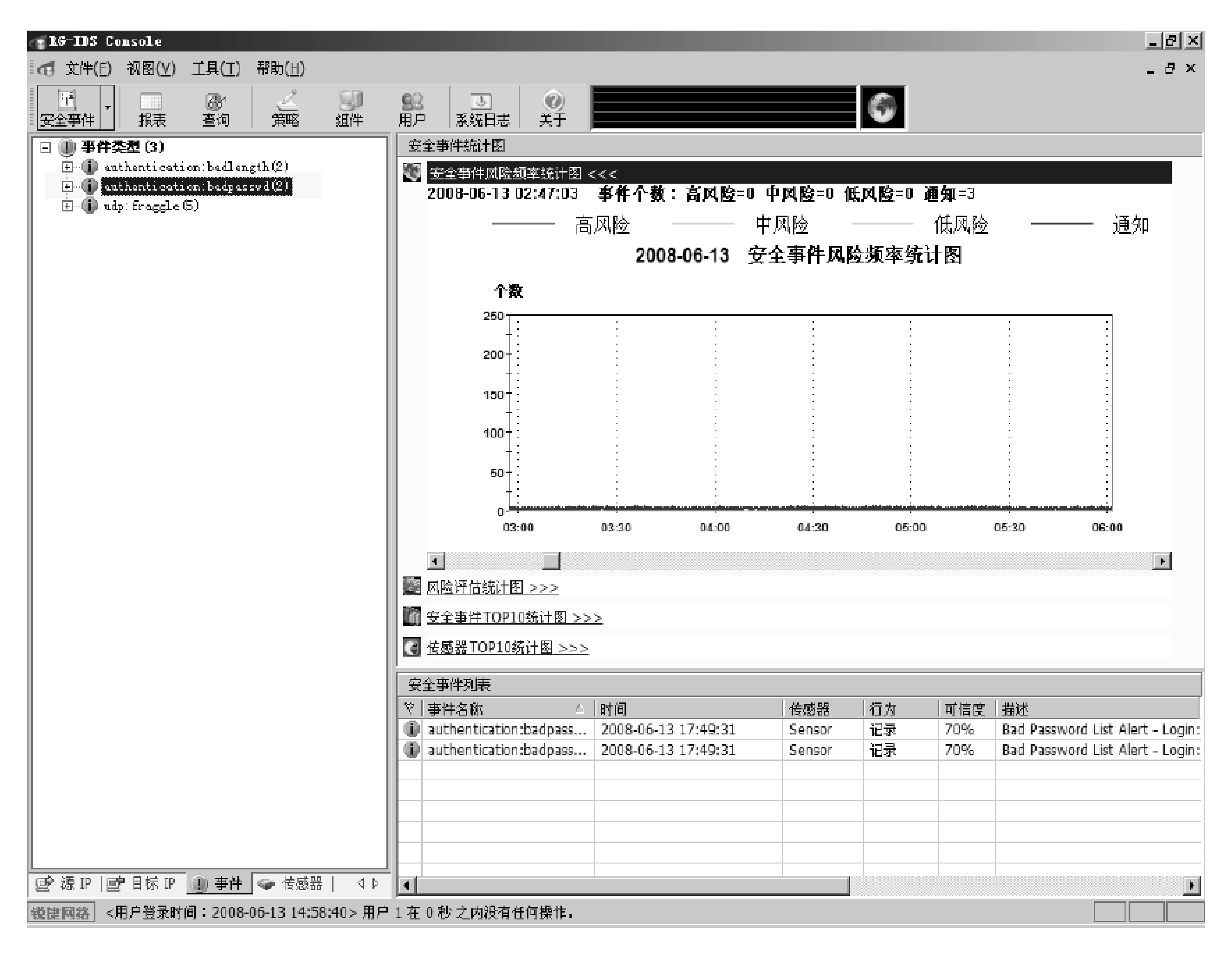



图 4-163 验证事件参数修改(1)




图 4-164 验证事件参数修改(2)

# 4.16 告警事件风暴抑制管理

## 【实验名称】

告警事件风暴抑制管理。

## 【实验目的】

通过本实验熟悉产品的操作,减少系统资源的消耗,对系统进行优化。

## 【背景描述】

某管理员通过系统的事件归并以及洪波抑制配置,从而减少同一安全事件上报的数量,达到优化系统的目的。

## 【需求分析】

短时间内某些安全告警事件大量上报,对系统资源造成极大的损耗。管理员通过系统的事件归并以及洪波抑制配置,达到优化系统的目的。

## 【实验拓扑】

如图 4-165 所示的网络拓扑,某企业网络管理员发现短时间内某些安全告警事件大量上报,对系统资源造成极大的损耗。因此,希望通过系统的事件归并以及洪波抑制配置,从而减少同一安全事件上报的数量,达到优化系统的目的,于是部署了 IDS 系统,配置告警事件风暴抑制管理,实现减少系统资源的消耗,对系统进行优化。

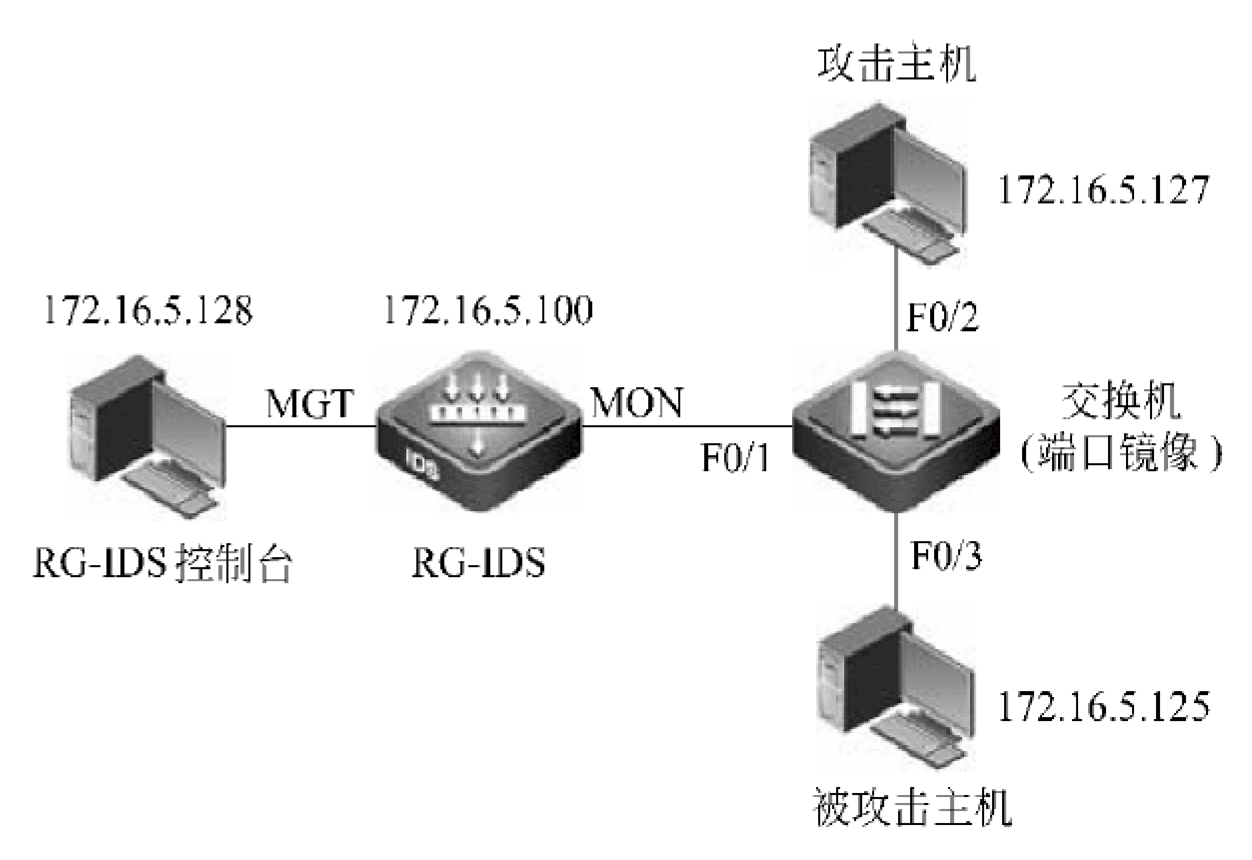



图 4-165　IDS 告警事件风暴抑制管理网络拓扑图

## 【实验设备】

PC　3 台
RG-IDS Sensor　1 台

直连线　　　　　4 条
交换机　　　　　1 台(支持多对一的端口镜像)

## 【预备知识】

RG-IDS 配置。

## 【实验原理】

事件归并配置：事件归并的整体配置是指针对所有安全事件签名设置一种默认的归并策略，这个归并策略将会作用在每一个传感器上，也就是说来自不同传感器的告警将不会被归并在一起。一旦开启这个功能，所有事件的默认归并策略即是该策略，但是即便用户开启了整体归并策略，也可以对每一个安全事件签名在"事件归并"设置中逐一修改归并策略。因此，该功能事实上是对没有设置归并策略的告警的整体配置。事件归并策略的内容包括：是否启用事件归并，默认按照事件名称归并(不可更改)，然后可以按照事件的源、目的地址和端口归并。事件归并个别配置指对于某一个或某几个攻击签名以及某一类攻击签名单独配置，系统只针对个别攻击签名进行归并。

洪波抑制：洪波抑制功能是指，如果短时间内大量相同的告警信息被发送给管理控制台，影响了用户对网络事件的分析，可以在洪波抑制界面设置洪波抑制功能，以防止短时间内产生大量相同的告警。

## 【实验步骤】

### 1. 事件归并配置

1）事件归并整体配置

如图 4-166 所示，进入"告警策略"窗口。右键单击"一般事件树"的树根节点 packages(也可以选中某个 Backend 或者 Package 节点配置，这样响应只针对该节点下面的子节点生效)。

在弹出的菜单中选择"事件归并整体配置"命令。在弹出的对话框中勾选"启用事件归并(对事件名称进行归并)"复选框，然后设置归并条件，如图 4-167 所示。

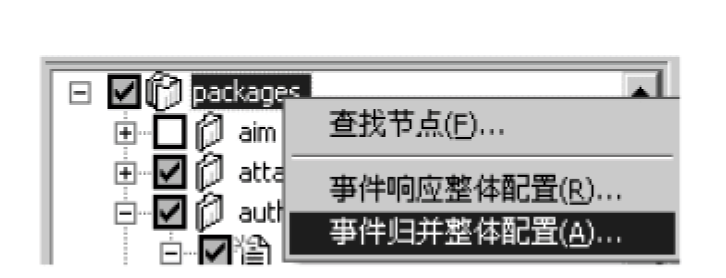



图 4-166　事件归并整体配置

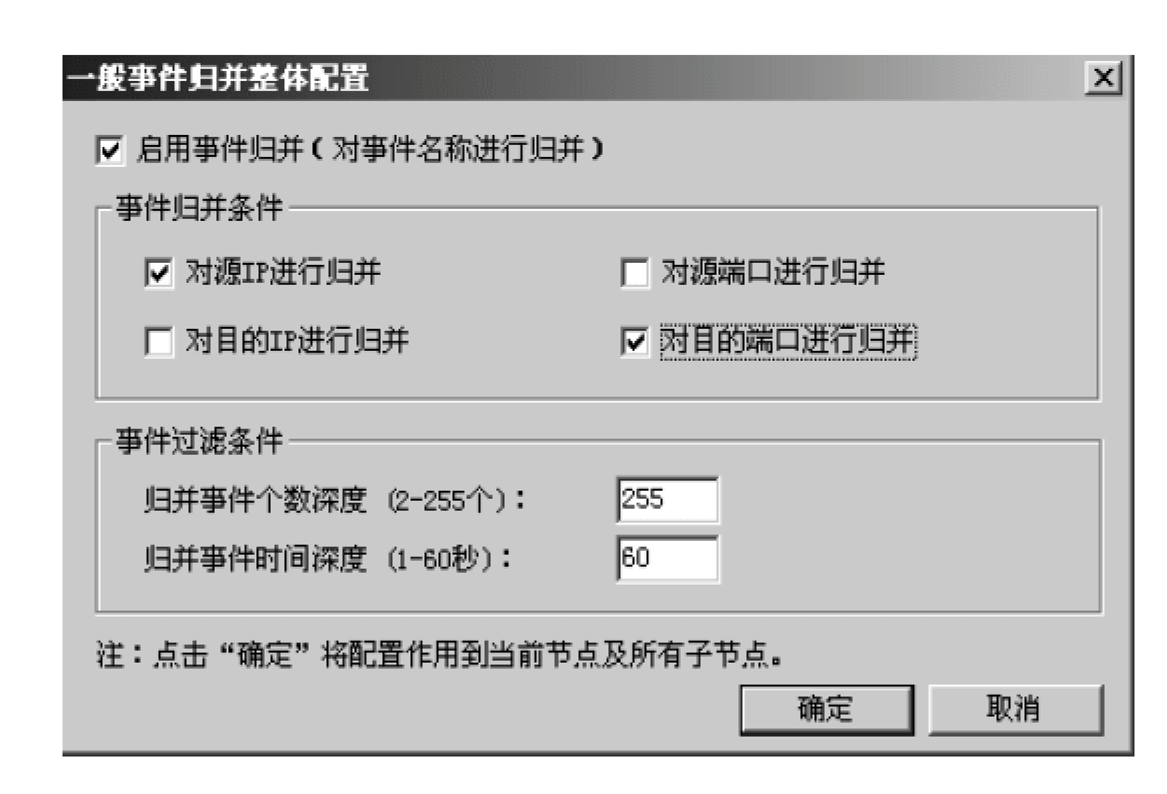



图 4-167　启用事件归并

单击“确定”按钮，事件归并整体配置就完成了。

2）事件归并个别配置

进入“告警策略”窗口。展开“一般事件树”，选中某一个攻击签名，在右侧的“事件归并”窗口中设置归并条件，如图 4-168 所示。

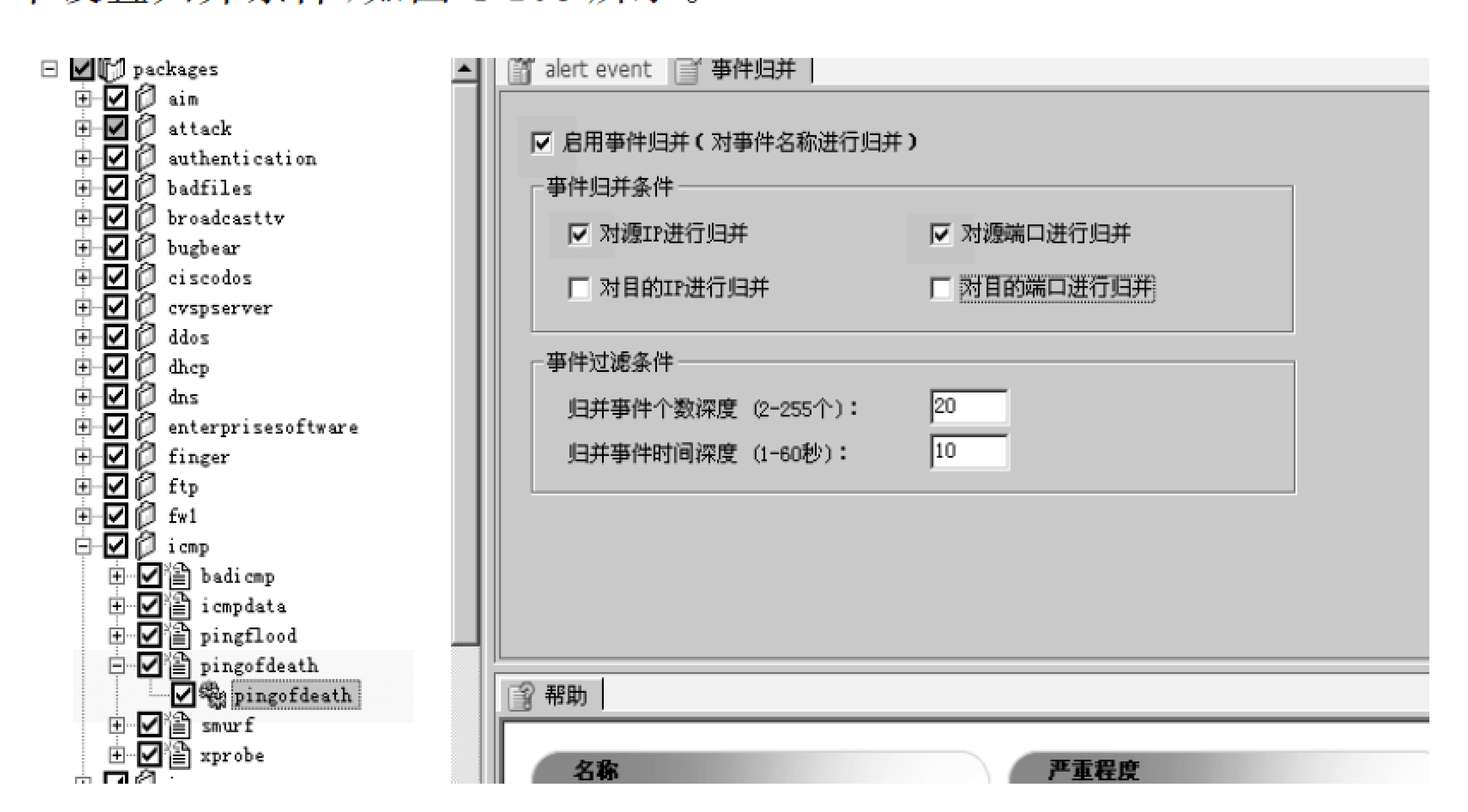



图 4-168　事件归并个别配置

## 2 验证事件归并配置

1）归并前后的事件信息

归并结果在表达上与非归并事件有一些细节差别。下面以 icmp：pingofdeath：pingofdeath_alert 事件为例进行说明。首先看看该事件的归并策略配置，如图 4-169 所示。




图 4-169　归并前后的事件信息

从图 4-169 中可以看到为 icmp：pingofdeath：pingofdeath_alert 事件配置的归并参数为“把来自相同的源 IP、源端口的同类事件划分为一组”。过滤条件是“当队列深度达到 20 时则触发归并产生结果”。归并前后事件的详细信息在窗口中会有明显差异。

icmp：pingofdeath：pingofdeath_alert 归并前的事件详细信息（在事件窗口双击事件）如图 4-170 和图 4-171 所示。

| ▽ | 事件名称 | 时间 | 传感器 | 行为 | 可... | 描述 | 通讯... | 源 IP | 源端口 | 目标 IP | 目标端口 | 数目 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | icmp:pingofdeath | 2008-0... | Sen... | 攻击 | 90% | 10.0.3.170 ->... | ICMP | 10.0.3.170 | 随机端口 | 10.0.3.67 | 随机端口 | 1 |
| | icmp:pingofdeath | 2008-0... | Sen... | 攻击 | 90% | 10.0.3.170 ->... | ICMP | 10.0.3.170 | 随机端口 | 10.0.3.67 | 随机端口 | 1 |
| | icmp:pingofdeath | 2008-0... | Sen... | 攻击 | 90% | 10.0.3.170 ->... | ICMP | 10.0.3.170 | 随机端口 | 10.0.3.67 | 随机端口 | 1 |
| | icmp:pingofdeath | 2008-0... | Sen... | 攻击 | 90% | 10.0.3.170 ->... | ICMP | 10.0.3.170 | 随机端口 | 10.0.3.67 | 随机端口 | 1 |
| | icmp:pingofdeath | 2008-0... | Sen... | 攻击 | 90% | 10.0.3.170 ->... | ICMP | 10.0.3.170 | 随机端口 | 10.0.3.67 | 随机端口 | 1 |
| | icmp:pingofdeath | 2008-0... | Sen... | 攻击 | 90% | 10.0.3.170 ->... | ICMP | 10.0.3.170 | 随机端口 | 10.0.3.67 | 随机端口 | 1 |

图 4-170　归并前的事件详细信息(1)




图 4-171　归并前的事件详细信息(2)

针对 icmp:pingofdeath:pingofdeath_alert 归并后的详细信息(在事件窗口双击事件),如图 4-172 和图 4-173 所示。

| ▽ | 事件名称 | 时间 | 传感器 | 行为 | 可... | 描述 | 通讯... | 源 IP | 源端口 | 目标 IP | 目标端口 | 数目 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | icmp:pingofdeath | 2008-0... | Sen... | 攻击 | 90% | 10.0.3.67 -> ... | ICMP | 10.0.3.67 | 随机端口 | 随机IP | 随机端口 | 12 |
| | icmp:pingofdeath | 2008-0... | Sen... | 攻击 | 90% | 10.0.3.67 -> ... | ICMP | 10.0.3.170 | 随机端口 | 随机IP | 随机端口 | 15 |
| | icmp:pingofdeath | 2008-0... | Sen... | 攻击 | 90% | 10.0.3.170 ->... | ICMP | 10.0.3.170 | 随机端口 | 10.0.3.67 | 随机端口 | 1 |
| | icmp:pingofdeath | 2008-0... | Sen... | 攻击 | 90% | 10.0.3.170 ->... | ICMP | 10.0.3.170 | 随机端口 | 随机IP | 随机端口 | 20 |
| | icmp:pingofdeath | 2008-0... | Sen... | 攻击 | 90% | 10.0.3.170 ->... | ICMP | 10.0.3.170 | 随机端口 | 10.0.3.67 | 随机端口 | 1 |
| | icmp:pingofdeath | 2008-0... | Sen... | 攻击 | 90% | 10.0.3.170 ->... | ICMP | 10.0.3.170 | 随机端口 | 随机IP | 随机端口 | 20 |

图 4-172　归并后的详细信息(1)

由于在定义归并策略时没有选择"对目的 IP 地址和目的端口进行归并",因此,同一分组中的事件可能是去往不同目的 IP 和不同的目的端口,为了避免歧义,在归并结果中目的地址和目的端口的统计信息被 0.0.0.0 和 0 替代。同时例如 LogDB 与防火墙互动等响应方式也不会出现在归并的结果中。

2) 归并前事件显示

启动"事件归并"功能前,所有事件全部罗列在事件窗口中,当事件风暴发生时,会对系统带来很大的压力,并会很快取缔其他告警信息。

3) 归并后事件显示

根据上面对 icmp:pingofdeath:pingofdeath_alert 设置归并参数后,启动"事件归并"功能,20 条事件类型相同的告警事件将被归并为一条事件,从而大大降低事件风暴对系




图 4-173　归并后的详细信息(2)

统的冲击。图 4-174 显示的事件数量为 12,因为在“事件过滤条件”中默认归并事件时间深度为 10 秒。当第一条事件产生后,10 秒内系统没有收到 20 条以上的事件,故系统将已收到的事件(12 条)归并为一条事件。另外,当某一事件第一次出现(或归并计数器复位),系统会立即将该事件提交并出现在事件窗口中,这样做的目的是消除事件归并对系统实时性的影响,如图 4-174 所示。

| 事件名称 | 时间 | 传感器 | 行为 | 可… | 描述 | 通讯… | 源 IP | 源端口 | 目标 IP | 目标端口 | 数目 |
|---|---|---|---|---|---|---|---|---|---|---|---|
| icmp:pingofdeath | 2008-0… | Sen… | 攻击 | 90% | 10.0.3.67 -> … | ICMP | 10.0.3.67 | 随机端口 | 随机IP | 随机端口 | 12 |
| icmp:pingofdeath | 2008-0… | Sen… | 攻击 | 90% | 10.0.3.67 -> … | ICMP | 10.0.3.170 | 随机端口 | 随机IP | 随机端口 | 15 |
| icmp:pingofdeath | 2008-0… | Sen… | 攻击 | 90% | 10.0.3.170 ->… | ICMP | 10.0.3.170 | 随机端口 | 10.0.3.67 | 随机端口 | 1 |
| icmp:pingofdeath | 2008-0… | Sen… | 攻击 | 90% | 10.0.3.170 ->… | ICMP | 10.0.3.170 | 随机端口 | 随机IP | 随机端口 | 20 |
| icmp:pingofdeath | 2008-0… | Sen… | 攻击 | 90% | 10.0.3.170 ->… | ICMP | 10.0.3.170 | 随机端口 | 10.0.3.67 | 随机端口 | 1 |
| icmp:pingofdeath | 2008-0… | Sen… | 攻击 | 90% | 10.0.3.170 ->… | ICMP | 10.0.3.170 | 随机端口 | 随机IP | 随机端口 | 20 |

图 4-174　归并后事件的显示

### 3. 洪波抑制配置

1）策略编辑

单击 RG-IDS 控制台主界面上的“策略”按钮,切换到策略编辑器界面,选择 attack:flood:flood_alert 以及 attack:flood: progress_alert 签名,如图 4-175 所示。

2）参数配置

根据实际情况对 attack:flood 下的参数进行配置,如图 4-176 所示。

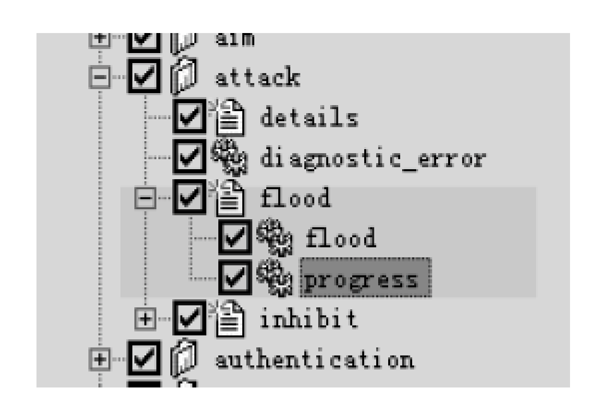
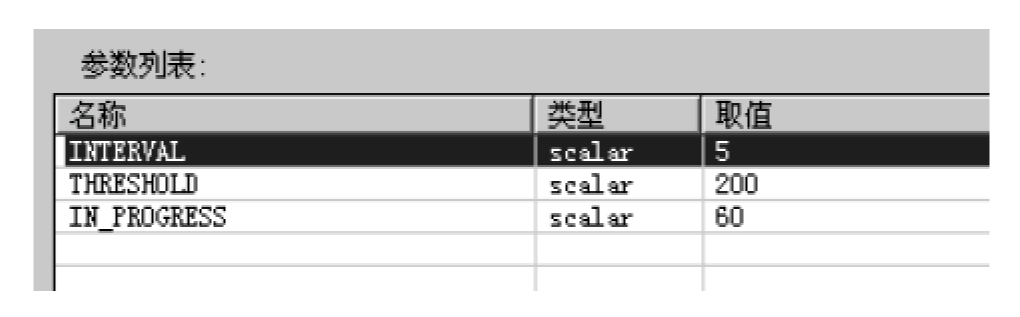



图 4-175　IDS 控制台策略编辑器界面


参数列表:

| 名称 | 类型 | 取值 |
|---|---|---|
| INTERVAL | scalar | 5 |
| THRESHOLD | scalar | 200 |
| IN_PROGRESS | scalar | 60 |

图 4-176　配置参数

**注意**：本实验所涉及的参数具体含义可参考相关的签名帮助文件。

## 4. 验证洪波抑制配置

以 icmp：pingofdeath：pingofdeath_alert 为例，洪波抑制开启前的告警信息，如图 4-177 所示。

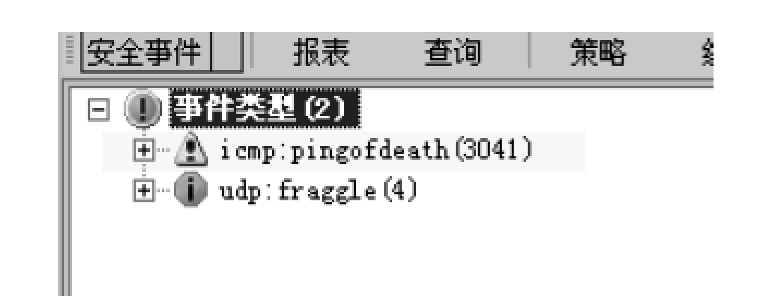



图 4-177　洪波抑制开启前的告警信息

洪波抑制开启后的告警信息，如图 4-178 和图 4-179 所示。

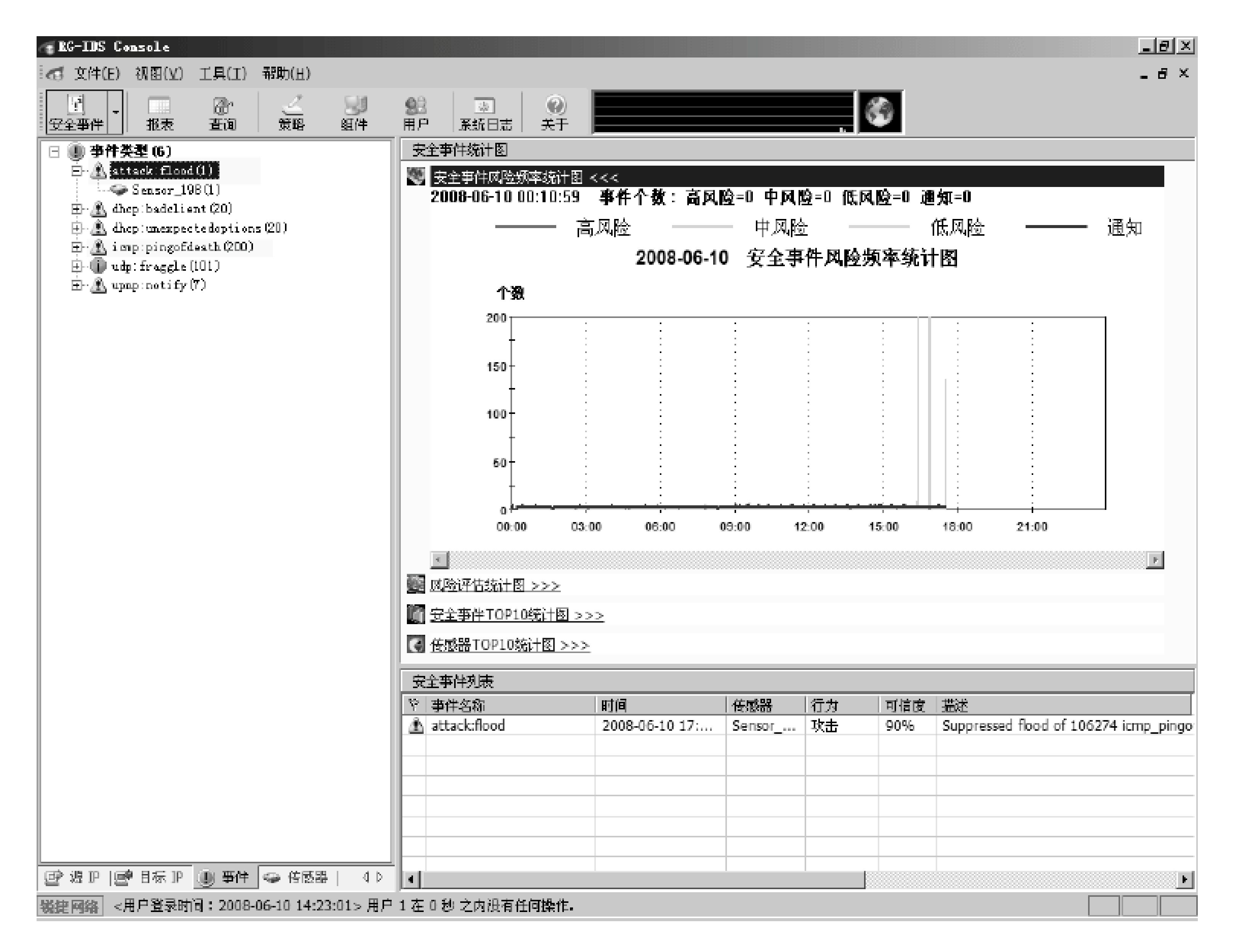



图 4-178　洪波抑制开启后的告警信息(1)




图 4-179　洪波抑制开启后的告警信息(2)

## 【注意事项】

事件归并针对的是从传感器发送到事件收集器的事件，而洪波抑制针对的是从事件收集器发送到管理控制台的告警事件。

# 4.17 事件响应方式管理

## 【实验名称】

事件响应方式管理。

## 【实验目的】

通过本实验熟悉产品的操作，熟悉对上报的安全事件的响应方式的处理。

## 【背景描述】

某管理员通过配置事件响应参数，当告警事件出现时，RG-IDS 会对此进行一系列的处理，如向管理员的邮箱发送事件警告等，使管理员能及时处理该突发事件。

## 【需求分析】

当一些突发的安全事件发生时，RG-IDS 会对告警做一系列的响应处理，如默认的"在控制台上显示"、"写入数据库保存"以及"发送 SNMP Trap"、"发送电子邮件通知"等，能及时地通知管理员。

## 【实验拓扑】

如图 4-180 所示的网络拓扑，某企业网络管理员发现通过配置事件响应参数，当告警

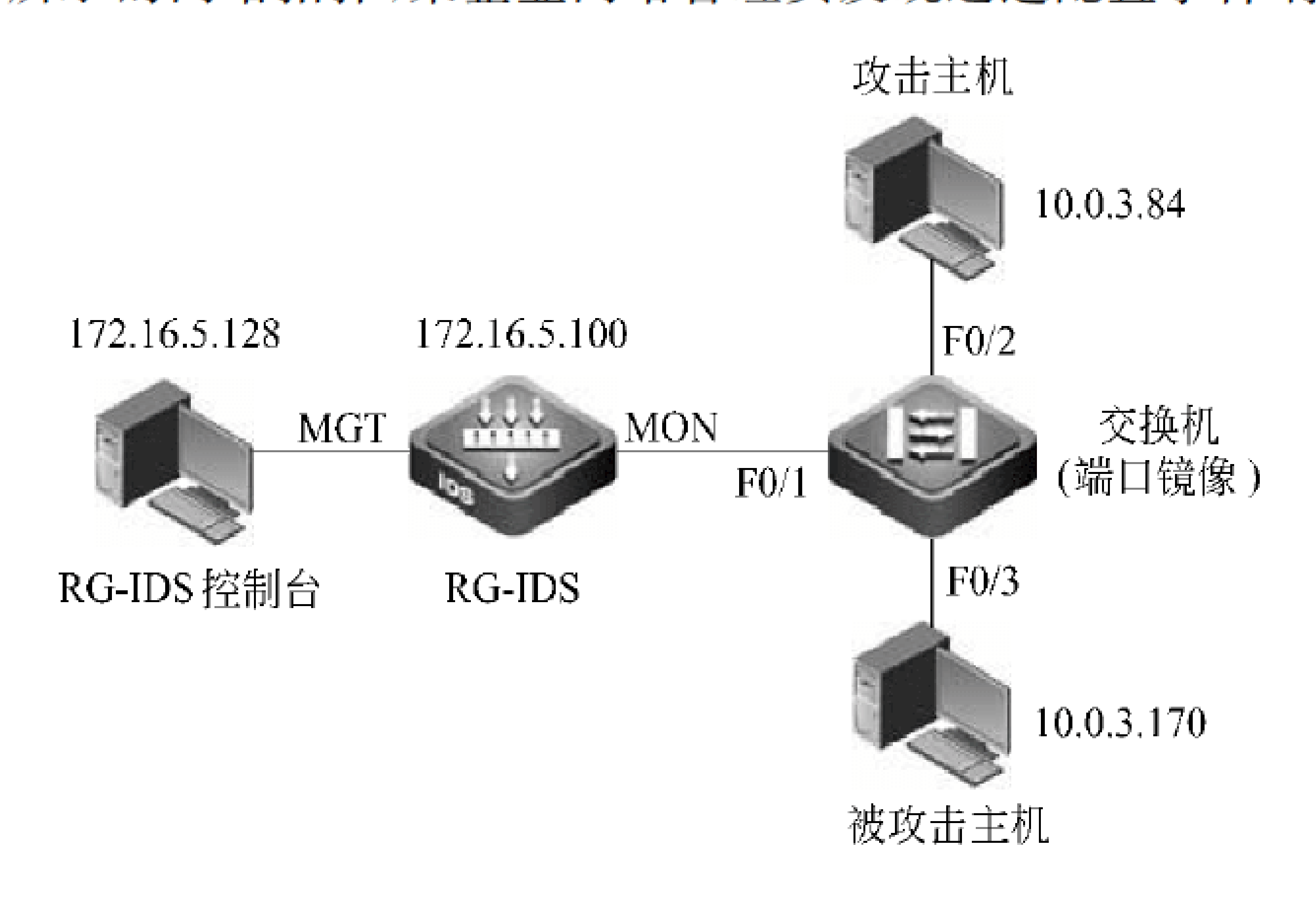



图 4-180　IDS 事件响应方式管理拓扑图

事件出现时，RG-IDS 会对此进行一系列的处理，如向管理员的邮箱发送事件警告等，使管理员能及时处理该突发事件，于是部署了 IDS 系统进行检测，加强对上报的安全事件的响应方式的处理防范功能。

## 【实验设备】

| | |
|---|---|
| PC | 3 台 |
| RG-IDS Sensor | 1 台 |
| 直连线 | 4 条 |
| 交换机 | 1 台（支持多对一的端口镜像） |

## 【预备知识】

RG-IDS 配置。

## 【实验原理】

在监测到安全事件后，系统管理平台可以根据所配置的策略进行以下响应：

- 将检测的事件显示在控制台上。
- 将检测的事件记录在数据库中。
- 发送 snmptrap。
- 在检测到特定事件时，通过电子邮件通知管理员。
- 在检测到特定事件时，运行用户指定的程序。

## 【实验步骤】

### 1. 响应参数设置

在响应参数设置窗口的左边是响应参数设置模板区域，响应参数设置模板类似告警策略模板。

在此区域可以对 SMTP、SNMP 等参数进行设置。本实验采取通过电子邮件通知管理员的响应策略，相关设置如图 4-181 所示。

### 2 事件响应个别配置

个别配置是指对于某一个或某几个攻击签名以及某一类攻击签名单独进行配置，系统只针对个别攻击签名进行响应。事件响应个别配置的步骤如下：

（1）进入“告警策略”窗口，如图 4-182 所示。

（2）展开“一般事件树”（对“特殊事件树”的操作与“一般事件树”相同）。

（3）选中某一个攻击签名，在右侧的响应窗口中选择响应方式（本实验以 icmp：pingofdeath：pingofdeath_alert 为例）。

保存策略并重新应用到传感器。




图 4-181　设置响应参数




图 4-182　事件响应个别配置

### 3. 验证事件响应配置

以 icmp:pingofdeath:pingofdeath_alert 为例，触发攻击后，事件上报到控制台并给管理员发出通知邮件，如图 4-183 和图 4-184 所示。

## 【注意事项】

除了对某个告警事件响应进行个别配置外，也可以对事件响应作整体配置，具体步骤如下：

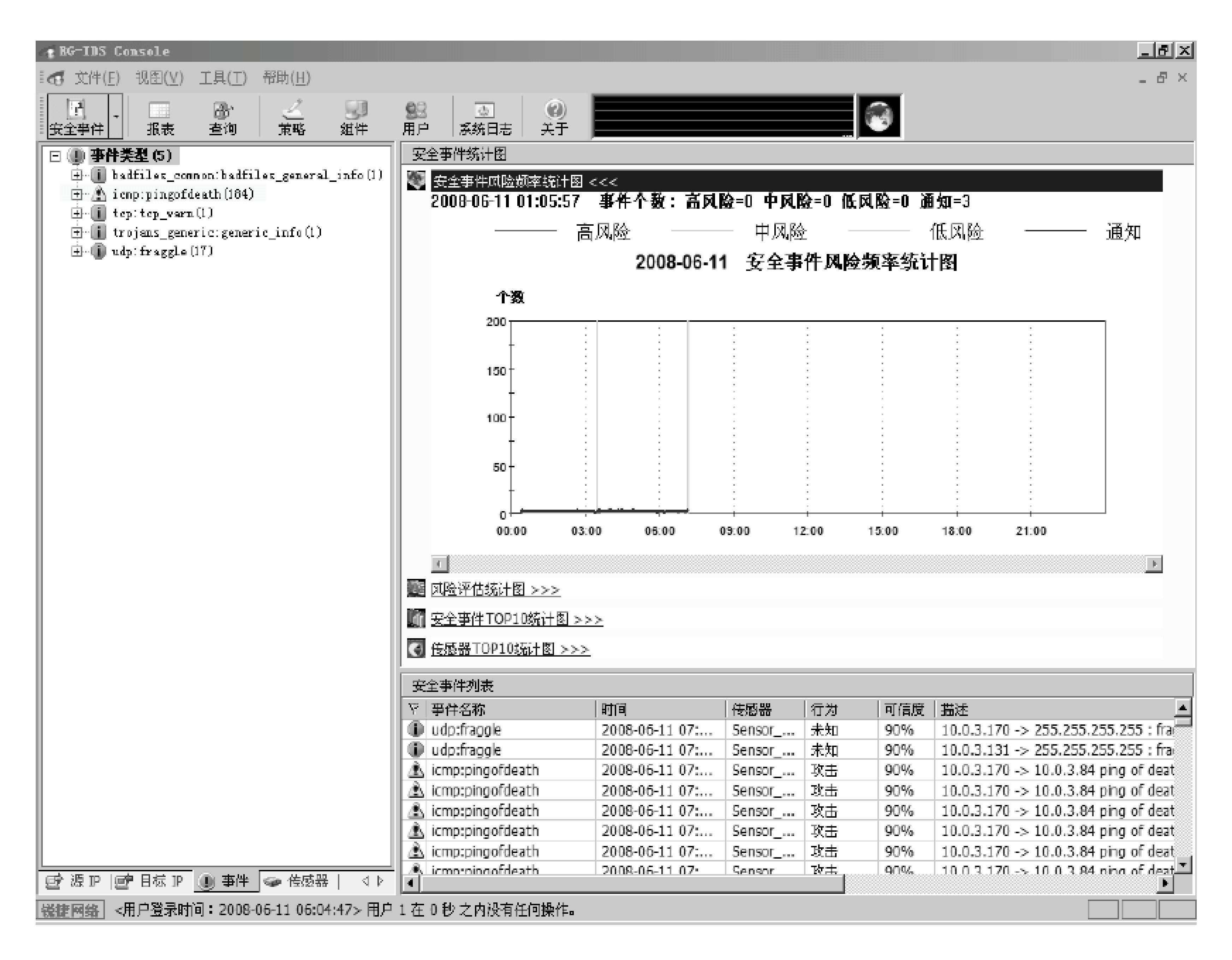



图 4-183 验证事件响应配置(1)

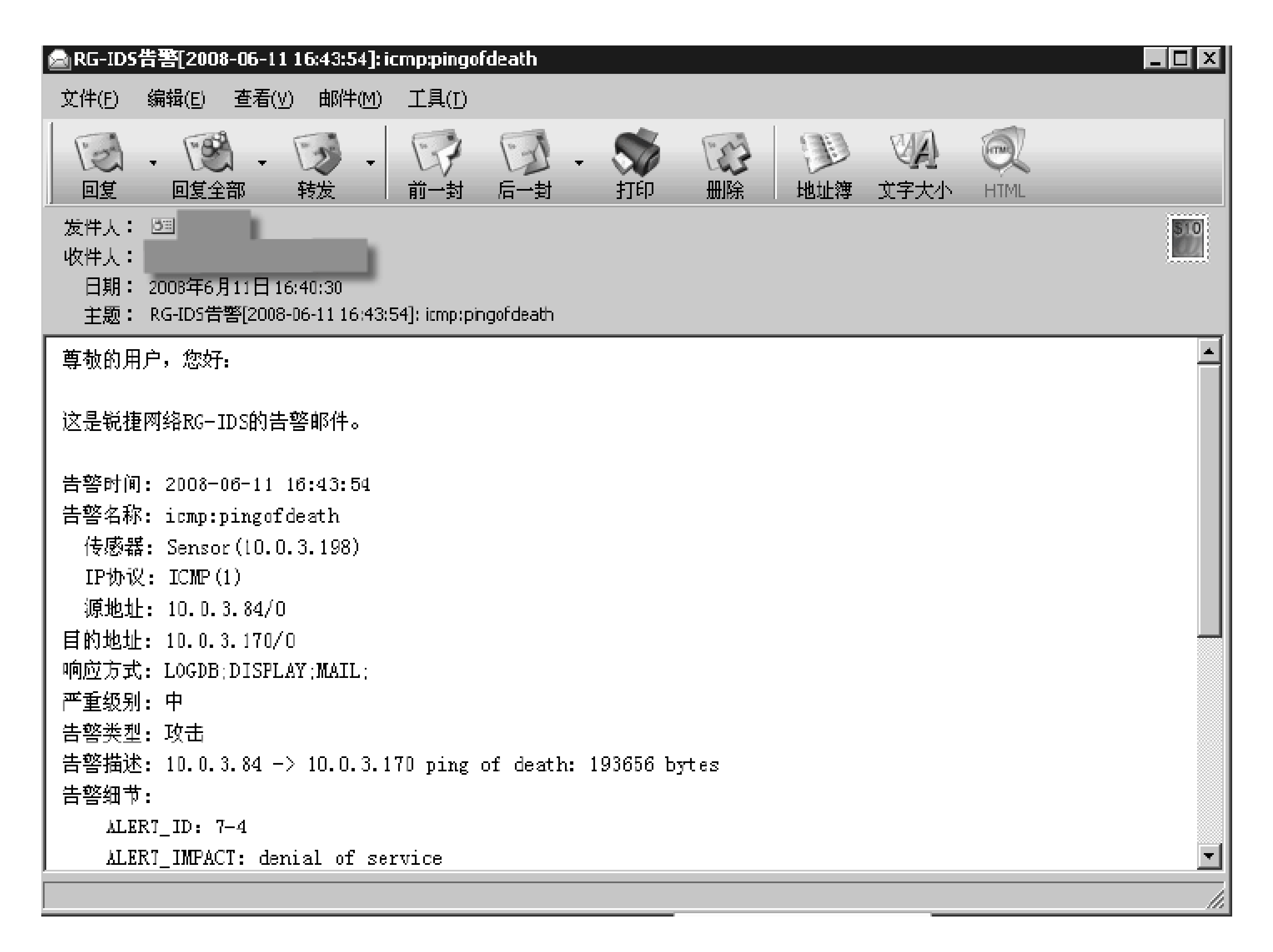



图 4-184 验证事件响应配置(2)

(1) 进入“告警策略”窗口，如图 4-185 所示。

(2) 右键单击“一般事件树”的树根节点 packages(也可以选中某个 Backend 或者 Package 节点配置，这样响应只针对该节点下面的子节点生效；对“特殊事件树”的操作与“一般事件树”相同)。

(3) 在弹出的菜单中选择“事件响应整体配置”命令。

(4) 在弹出的窗口中选中需要的响应方式，如图 4-186 所示。

图 4-185　配置告警策略

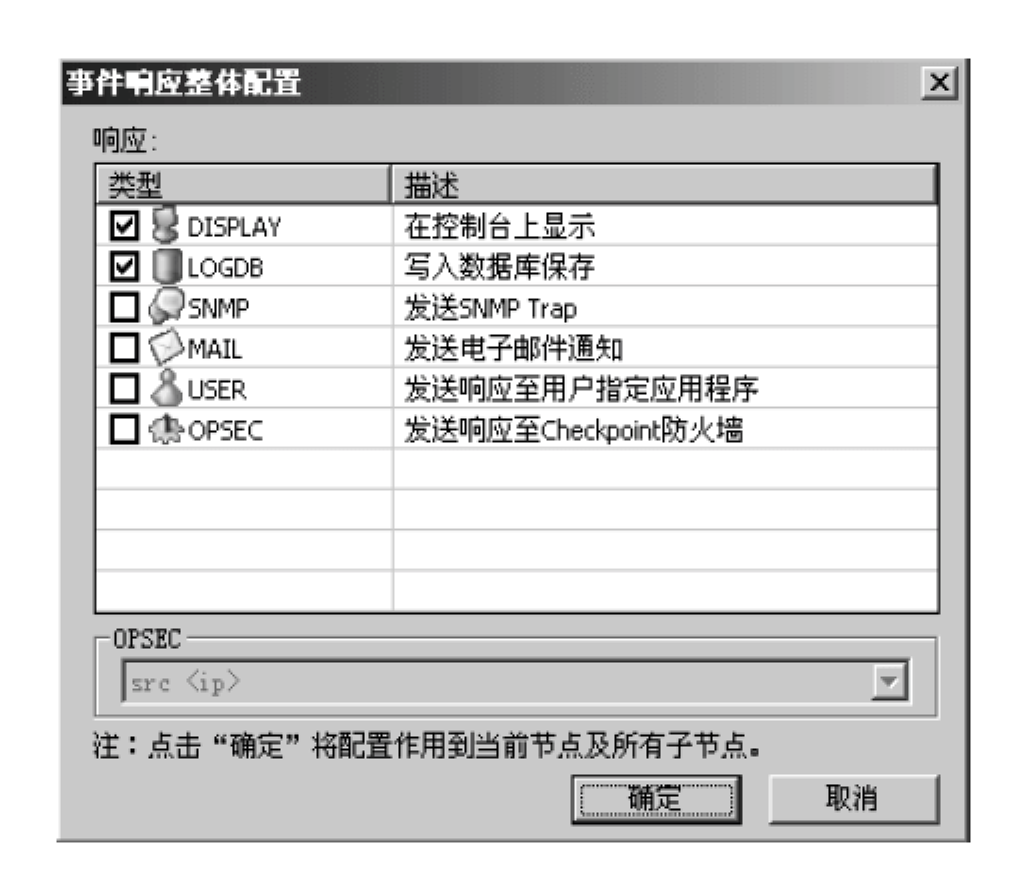



图 4-186　选中需要的响应方式

# 4.18　RG-IDS 报表管理

## 【实验名称】

RG-IDS 报表管理。

## 【实验目的】

掌握报表工具的管理与使用。

## 【背景描述】

某用户根据实际网络环境进行报表管理器的配置管理。

## 【需求分析】

用户需要使用报表查看工具，对报表进行查看和管理。

## 【实验拓扑】

如图 4-187 所示的网络拓扑，某企业网络管理员根据实际网络环境进行报表管理器的配置管理，于是部署了 IDS 系统进行检测，实现报表查看工具对报表进行查看和管理功能。

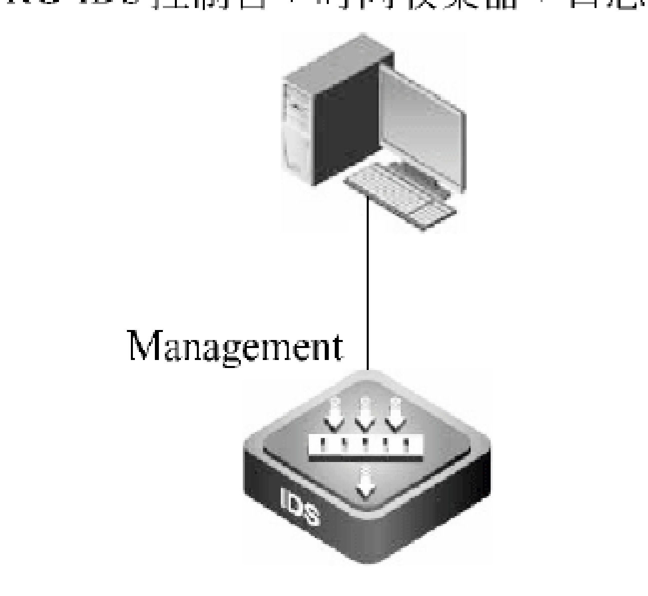



图 4-187　RG-IDS 报表管理网络拓扑图

## 【实验设备】

| | |
|---|---|
| PC | 1 台 |
| RG-IDS Sensor | 1 台 |
| 直连线 | 1 条 |

## 【预备知识】

RG-IDS 配置。

## 【实验原理】

Report 子系统作为 RG-IDS 系统的一个独立的部分，主要完成从数据服务器提取数据进行显示的功能。

## 【实验步骤】

### 1. 登录报表管理器

单击报表按钮，进入登录报表管理器界面。输入相应的账号、密码(前提是该账号拥有报表管理权限)以及事件收集器和数据服务器的 IP 地址，如图 4-188 所示。




图 4-188　登录报表管理器界面

登录成功后如图 4-189 所示。

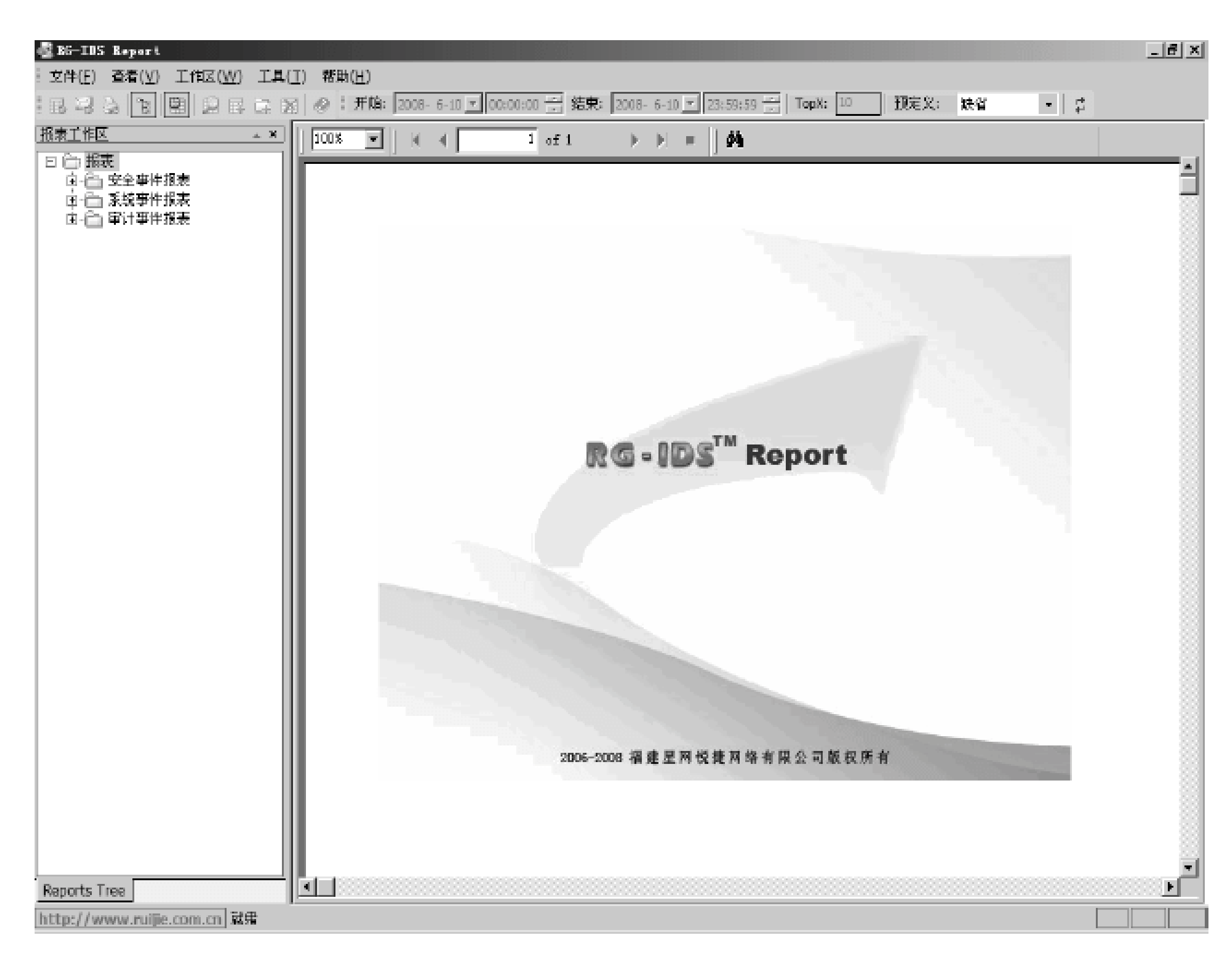



图 4-189　成功登录报表管理器

## 2 报表查看

依次选择报表工作区中的“报表”→“安全事件报表”→“告警类别统计”→“周告警类别统计”选项，在报表显示区内显示“告警类别—周统计信息”的柱状图和饼状图，如图 4-190 所示。

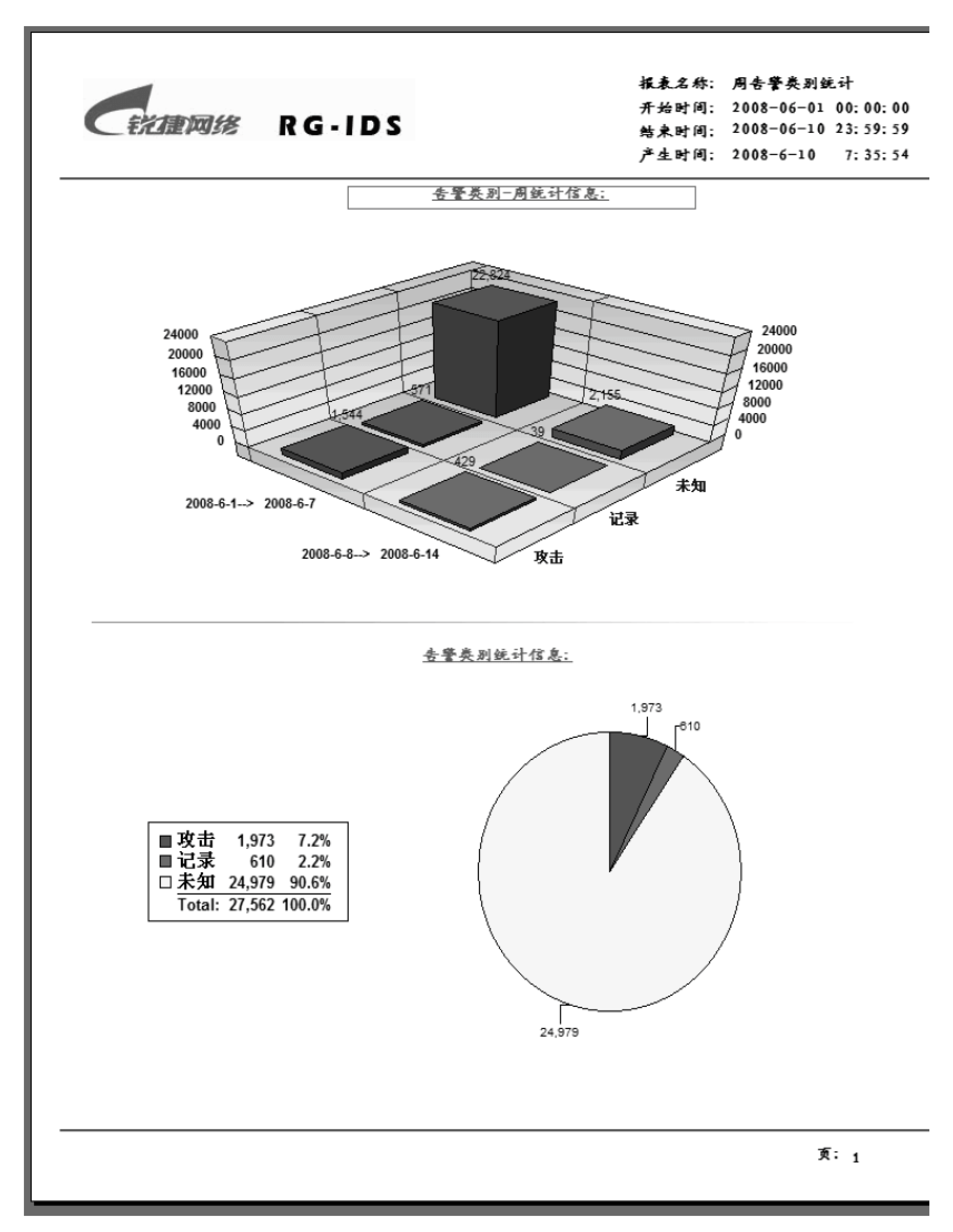



图 4-190　查看报表

## 3. 导出报表

选择报表主窗口“文件”→“导出报表”选项，在弹出的窗口中选择保存路径，输入保存名称，选择保存格式(可以保存为 4 种格式，如“. rpt”、“. txt”、“. html”和“. rtf”)，如图 4-191 所示。




图 4-191 导出报表文件

## 【注意事项】

如果登录报表管理器提示超时,有可能是由于个人防火墙的配置造成的,请正确配置防火墙。

# 4.19 RG-IDS 数据库管理

## 【实验名称】

RG-IDS 数据库管理。

## 【实验目的】

使用查询工具熟悉事件查询的方式,并对数据库进行管理和维护。

## 【背景描述】

某管理员需要对数据库进行管理、查询以及数据库备份、恢复、导出、同步等操作。

## 【需求分析】

RG-IDS 的安全、审计、统计、系统事件都存放在数据库中,并且提供了一整套强大的工具,以便管理员对数据库进行管理、查询以及数据库备份、恢复、导出、同步等操作。

## 【实验拓扑】

如图 4-192 所示的网络拓扑,某企业网络管理员需要对数据库进行管理、查询以及数据库备份、恢复、导出、同步等操作,于是部署了 IDS 系统,使用查询工具熟悉事件查询的方式,并对数据库进行管理和维护。

RG-IDS控制台、时间收集器、日志服务器

Management

IDS

图 4-192 RG-IDS 数据库管理网络拓扑图

## 【实验设备】

PC　　1 台
RG-IDS Sensor　　1 台
直连线　　1 条

## 【预备知识】

RG-IDS 基本配置。

## 【实验原理】

通过查询工具对数据库进行查询，并使用数据库维护工具对数据库进行维护和管理。

## 【实验步骤】

### 1. 数据的管理和查询

1）登录查询工具管理器

单击 查询 按钮，进入查询工具管理器登录界面，输入相应的账号、密码（前提是该账号拥有数据查询权限）以及事件收集器的 IP 地址，如图 4-193 所示。




图 4-193　登录查询工具管理器界面

登录成功，界面如图 4-194 所示。

2）添加日志服务器

单击 添加 按钮，添加日志服务器，如图 4-195 所示。

添加成功后如图 4-196 所示。

3）添加查询

设置相应的查询条件，如图 4-197 所示。

单击“条件预览”按钮，确认查询条件无误后单击“确定”按钮，如图 4-198 所示。

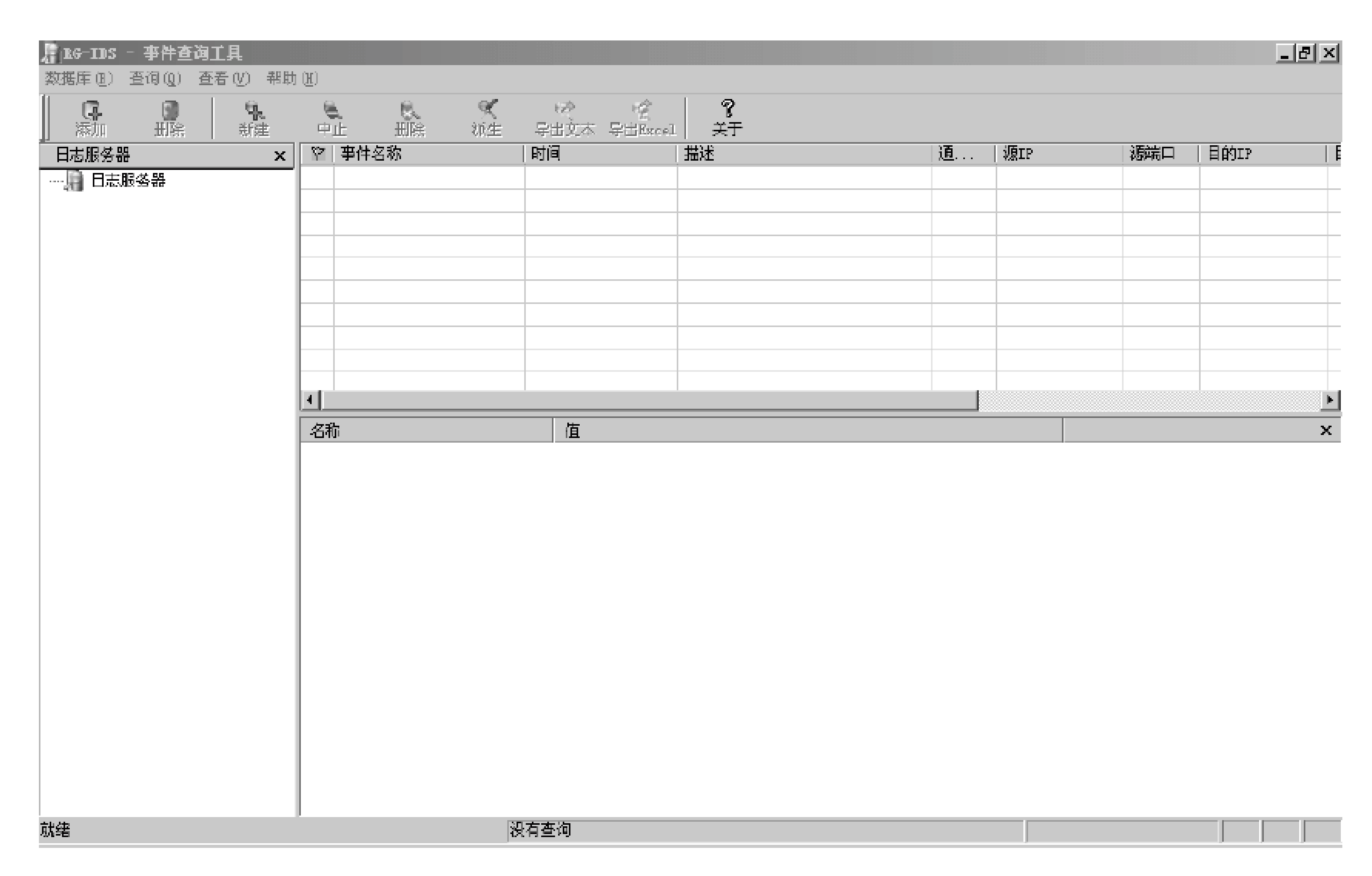



图 4-194　成功登录查询工具管理器




图 4-195　添加日志服务器

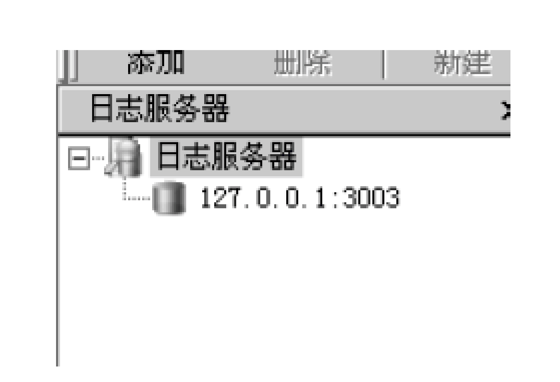



图 4-196　成功添加日志服务器




图 4-197　相应的查询条件




图 4-198　确认查询条件

查询工具窗口右上方是查询结果的摘要显示。用户在日志服务器树上选择不同节点，右边列表会随之修改，而用户在摘要窗口选择事件，它的详细信息列表会在右下窗口显示，完全相同的详细信息会被归并为一条，并以“事件产生时间(个数)”的形式显示每一条详细信息的名称，如图 4-199 所示。

| | 事件名称 | 时间 | 描述 | 通... | 源IP | 源端口 | 目的IP | 目 |
|---|---|---|---|---|---|---|---|---|
| i | badfiles_common:badf... | 2008-06-09 23:5... | File Parsing : NOTICE: WWW2 ... | N/A | 随机IP | 随机端口 | 随机IP | 随 |
| i | badfiles_common:badf... | 2008-06-09 22:4... | File Parsing : NOTICE: WWW2 ... | N/A | 随机IP | 随机端口 | 随机IP | 随 |

图 4-199　查询结果的摘要显示

查询工具窗口右下方是查询结果信息，如图 4-200 所示。

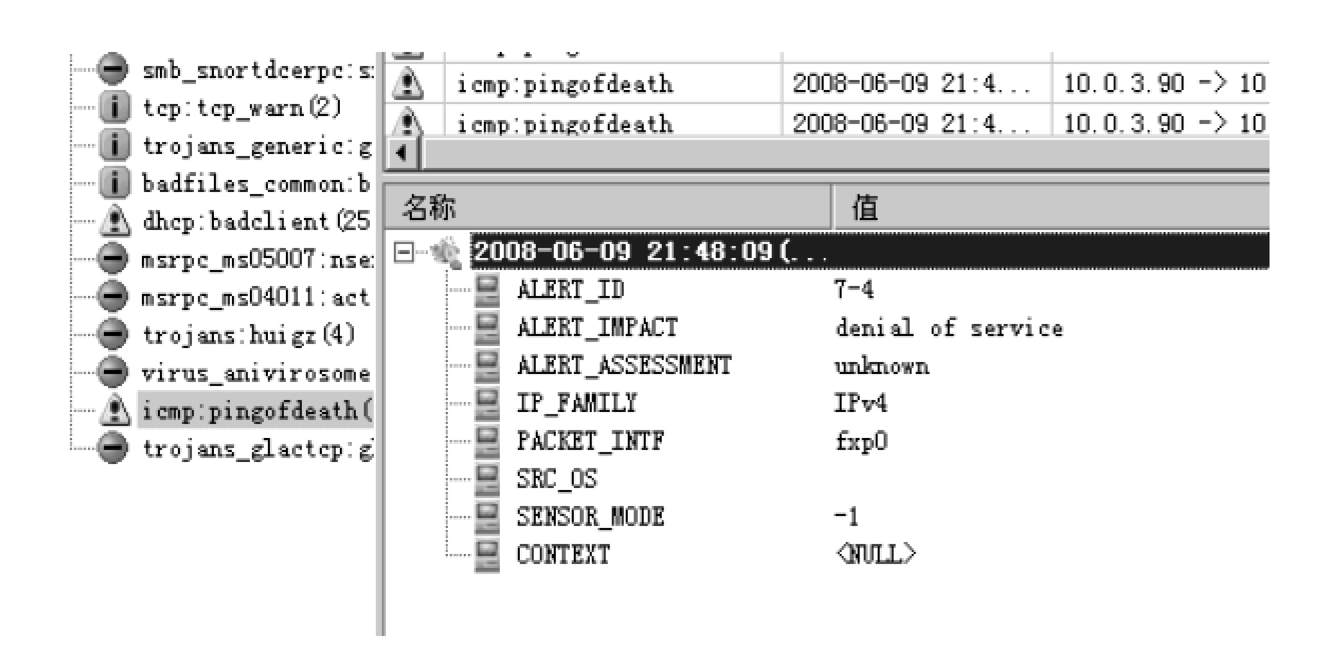



图 4-200　查询结果信息

## 2 数据库维护

1）登录“LogServer 数据库维护工具”

如图 4-201 所示，依次选择“开始”→“程序”→“锐捷入侵检测系统”→“锐捷入侵检测系统(网络)”→“RG-IDS 数据库维护工具”选项。在登录框中输入相应的账号、密码。




图 4-201　登录 LogServer 数据库维护工具

2）数据库维护(以备份为例说明)

进入“LogServer 数据库维护工具”，选择相应的数据类型(本例选择“安全事件”)，在维护操作中选择“备份”，以及起始时间和相应的文件路径，单击“开始”按钮，如图 4-202 所示。

备份成功后，如图 4-203 和图 4-204 所示。




图 4-202　数据库维护备份




图 4-203　成功备份数据库(1)




图 4-204　成功备份数据库(2)







# 第3篇 统一安全网关安全

# 第 5 章 统一安全网关基础知识

随着网络技术的快速发展,各种网络威胁也在不断出现,安全漏洞的频频曝光,黑客技术的日新月异,木马蠕虫等病毒的不断变种,导致很多企业用户谈“网”色变。

网络安全威胁已成为每个企业亟待解决的问题,面对多变的网络攻击,采用防火墙、入侵检测、防病毒等安全设备是传统大型企业的首选,但这些设备费用高,日常维护工作复杂技术,让很多中小企业望而却步,USG(统一安全网关)的出现,为这些中小企业带来了新的选择。

## 5.1 什么是统一安全网关

防火墙、IDS、防病毒技术经过多年发展,现在已经逐渐成熟并稳定,开始相互渗透,相互补充。近两年,出现了一个明显的趋势:防火墙、IDS、防病毒甚至内容过滤厂商分别从自有产品出发,通过增加不同的安全功能模块来发展 USG。实际上,这主要得益于硬件技术的发展。为了解决深度检查大量耗费 CPU 资源,除 ASIC 加速芯片外,一批新的硬件解决方案出现了,这些硬件能大幅度加速内容匹配,使 USG 从概念变成了可用的产品。

统一安全网关(Unified Securty Gatway,USG)技术就是将防病毒、入侵检测和防火墙安全设备划归统一安全网关新类别。目前,USG 常定义为由硬件、软件和网络技术组成的具有专门用途的设备,简单来说它就是将多项安全功能和多种安全特性集成在一个硬件设备中,构成一个标准的统一管理平台,如图 5-1 所示。USG 主要提供一项或多项安全功能,同时将多种安全特性集成在一个硬件设备中,形成标准的统一安全网关管理平台。从 USG 定义可以看出,USG 集中了多种安全功能,但这些安全功能不一定同时应用,可以只使用某一个功能。因此,USG 完全有可能取代防火墙、网络入侵检测等单一功能的安全产品。

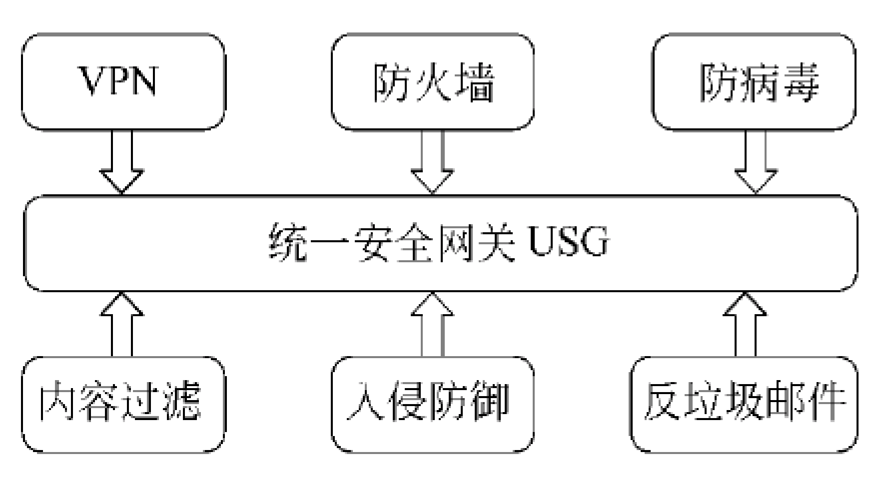


图 5-1　统一安全网关管理平台

USG 设备应该具备的基本功能包括网络防火墙、网络入侵检测/防御和网关防病毒功能。USG 集成了多种功能,但却不一定要同时开启。根据不同用户的不同需求以及不同的网络规模,USG 产品分为不同的级别。也就是说,如果用户需要同时开启多项功能,则需要配置性能比较高、功能比较丰富的产品。

## 5.2 统一安全网关特点

USG集多功能于一身,除了传统的防火墙功能外,入侵防御(IPS)功能的加入使得USG的防御能力达到2~7层;防病毒功能为企业的数据安全提供了保障;端到端的IPSec VPN功能为大中型企业扩展业务带来了便利;动态路由功能为公司节省了投资;内容过滤功能更是消除了页面、URL、网页控件等带来的威胁;借助入侵防御引擎的深度扫描能力使反垃圾邮件功能更加强大。强大的综合性能使得很多企业开始选择USG,高度集成化的趋势正在安全产品领域形成。

也许有人会指出USG是一个完整的安全硬件,一旦出现问题可能会导致所有安全防御功能失效,造成无法挽回的损失。对于这个问题用户大可放心,因为现在的USG已具备高可用性,能够采用主备模式,在检测到链路和设备故障时由备份设备取代主设备,提供不间断的安全防护,保证企业网络的安全稳定。

统一安全网关USG在组建安全网络中的优点如下:

(1) 整合所带来的成本降低

将多种安全功能整合在同一产品中能够让这些功能组成统一的整体发挥作用,相比于单个功能的累加功效更强,颇有一加一大于二的意味。现在很多组织特别是中小企业用户受到成本限制而无法获得令人满意的安全解决方案,USG产品有望解决这一困境。包含多个功能的USG安全设备价格比单独购买这些功能要低,这使得用户可以用较低的成本获得相比以往更加全面的安全防御设施。

(2) 降低信息安全工作强度

由于USG安全产品可以一次性获得以往多种产品的功能,并且只要插接在网络上就可以完成基本的安全防御功能,所以在部署过程中可以大大降低强度。另外,USG安全产品的各个功能模块遵循同样的管理接口,并具有内建的联动能力,所以在使用上也远比传统的安全产品简单。同等安全需求条件下,USG安全设备的数量要低于传统安全设备,无论是厂商还是网络管理员都可以减少服务和维护工作量。

(3) 降低技术复杂度

由于在USG安全设备中装入了很多的功能模块,所以为提高易用性进行了很多考虑。另外,这些功能的协同运作降低了掌握和管理各种安全功能的难度以及用户误操作的可能。对于没有专业信息安全人员及技术力量相对薄弱的组织来说,使用USG产品可以提高这些组织应用信息安全设施的质量。

统一安全网关USG在组建安全网络中的缺点如下:

(1) 网关防御的弊端

网关防御在防范外部威胁时非常有效,但是在面对内部威胁时就无法发挥作用了。有很多资料表明造成组织信息资产损失的威胁大部分来自于组织内部,所以以网关型防御为主的USG设备目前尚不是解决安全问题的万灵药。

(2) 过度集成带来的风险

将所有功能集成在 USG 设备当中使得抗风险能力有所降低。一旦该 USG 设备出现问题,将导致所有的安全防御措施失效。USG 设备的安全漏洞也会造成相当严重的损失。

(3) 性能和稳定性

尽管使用了很多专门的软硬件技术用于提供足够的性能,但是在同样的空间下实现更高的性能输出还是会对系统的稳定性造成影响。目前 USG 安全设备的稳定程度相比传统安全设备来说仍有很多需要改进的地方。

## 5.3 统一安全网关设备

RG-USG200 采用高性能的硬件架构和一体化的软件设计,集防火墙、VPN、入侵防御(IPS)、防病毒、外联控制、抗拒绝服务攻击(Anti-DoS)、内容过滤、反垃圾邮件、NetFlow 等多种安全技术于一身,同时全面支持 QoS、高可用性(HA)、日志审计等功能,为网络边界提供了全面实时的安全防护,如图 5-2 所示。



图 5-2 统一安全网关设备

RG-USG200 统一集成防火墙/VPN/安全路由器/安全交换机系统,提供百兆性能、模块化架构、WiFi 接入和丰富的路由器、交换机功能,带 2 个固定的 Untrust 10/100 接口和 4 个固定的 Trust 10/100 接口,并附加 1 个 MIC 扩展插槽,可以灵活扩展广域网或局域网接口。还额外支持一个 Express 接口,专门用来扩展 3G 接口。

# 第 6 章 统一安全网关实践技术

## 6.1 统一安全网关初始化配置

### 【实验名称】

统一安全网关初始化配置。

### 【实验目的】

登录 USG(统一安全网关)设备管理界面,进行基本的初始化配置。

### 【背景描述】

某企业为了提高网络的安全性,购买了一台 RG-USG 统一安全网关,现在需要登录到 USG 并对其进行基本配置。

### 【需求分析】

网络管理员需要对 USG 进行基本的配置。

### 【实验拓扑】

如图 6-1 所示的网络拓扑,是企业为了提高网络的安全,购买的一台 RG-USG 统一安全网关,现在需要登录到 USG 并对其进行基本配置,以实现网络的安全防范功能。

管理主机
192.168.1.200/24
Eth0
192.168.1.250/24
USG

图 6-1 统一安全网关初始化配置网络拓扑图

### 【实验设备】

USG 1 台
PC 1 台

### 【预备知识】

- 网络基础知识。
- USG 操作基础知识。

### 【实验原理】

USG 支持使用 Web 方式进行管理,所有的管理流量都是通过 SSL 进行加密的,并且

只有通过身份认证后才能登录到管理界面,并进行后续的配置。

## 【实验步骤】

### 1. 登录 USG的 Web管理界面

在默认出厂配置中,USG 的 Eth0 接口预先配置了 IP 地址 192.168.1.250/24,所以在本实验中使用地址为相同子网的管理主机 192.168.1.200/24 连接到 Eth0 接口对 USG 进行管理。

USG 使用 HTTPS 对管理流量进行加密。在浏览器地址栏中输入 https://192.168.1.250,浏览器将提示是否接受 USG 证书,单击“是”按钮, 如图 6-2 所示。




图 6-2　登录 USG 的 Web 管理界面

接受证书后,进入 USG 登录界面,默认的用户名为 admin,密码为 ruijie.USG, 如图 6-3 所示。

单击“登录”按钮后,进入 USG Web 管理界面。在这里可以查看系统的版本信息、系统资源的使用率等, 如图 6-4 所示。

### 2. 添加管理员

USG 出厂默认的管理员为 admin,密码为 ruijie.USG,为了提高安全性,推荐对默认管理员的密码进行修改,也可以添加更多的管理员。

进入“管理员”页面, 如图 6-5 所示。

单击“新建”按钮添加管理员。在“访问权限”下拉列表中指定该管理员所绑定的权限列表,安全列表在“管理员权限表”页面中进行配置。如果要限制该管理员可以登录 USG 所使用的 IP 地址,在“高级选项”区域通过地址/掩码的形式输入地址信息,如图 6-6 所示。




图 6-3 登录 USG 账户信息




图 6-4 进入 USG Web 管理界面




图 6-5 添加管理员账号

新建管理员

用户名　testuser

描述

访问权限　admin

密码

密码　●●●●●●

确认密码　●●●●●●

RADIUS

高级选项

管理IP/掩码 #1　192.168.1.100/32

管理IP/掩码 #2

管理IP/掩码 #3

提交　取消

图 6-6　添加管理员访问权限

选择“管理员权限表”选项卡，可以配置管理权限列表，默认的管理权限列表为 admin，如图 6-7 所示。




图 6-7　配置管理权限列表

单击“新建”按钮后可以创建权限列表，并指定该列表所具有的权限，如图 6-8 所示。

### 3. 配置接口

进入“接口”页面。在这里单击“新建”按钮创建 VLAN 接口，或单击现有接口列表中最右侧的“编辑”图标对接口进行配置，如图 6-9 所示。

单击接口最右侧的“编辑”图标，进入“接口”页面。这里可以为接口指定 IP 地址信息，或者将接口配置为使用 DHCP 或 PPPoE 的方式获取地址。

如果该接口可以作为管理接口，可以在“管理访问”区域指定允许的管理方式和是否允许 ping 该接口的地址。

在“高级选项”区域还可以指定接口的 MTU、协商模式等参数，如图 6-10 所示。




图 6-8　创建权限列表

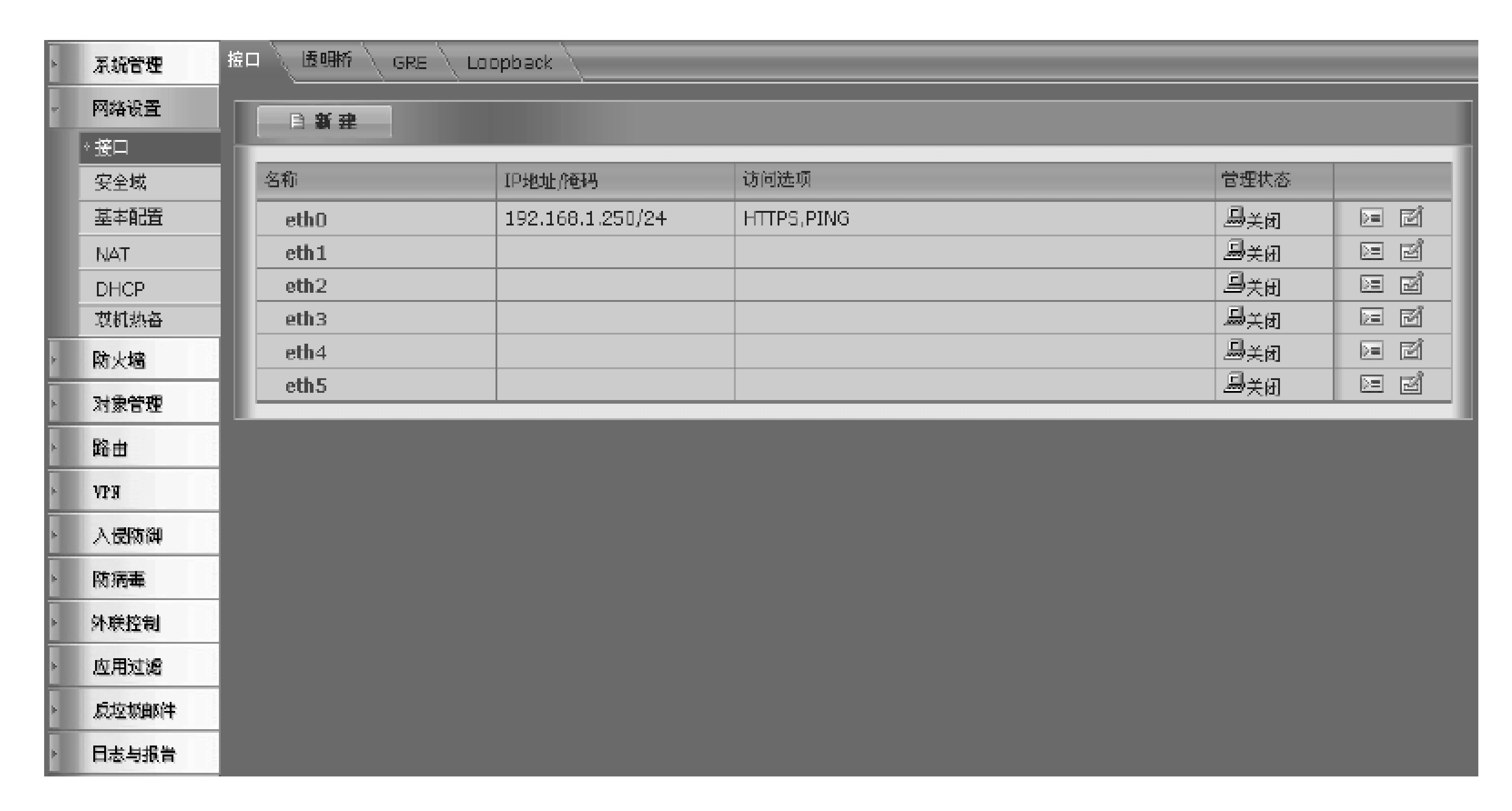



图 6-9　配置接口




图 6-10　配置接口信息

### 4. 配置安全域

安全域是指 USG 所连接的网络区域,可以将接口加入到安全域中,然后在各种策略中使用安全域。安全域的配置不是必需的,但是当 USG 通过多个接口连接到多个网络时,推荐使用安全域进行划分,这样可以方便后续策略的配置。通常连接内部网络的接口将划分到一个安全域,连接外部网络(例如 Internet)的接口划分到一个安全域。根据网络的拓扑结构,还可以划分多个安全域。

进入“安全域”页面,默认不存在安全域,如图 6-11 所示。




图 6-11　配置安全域

单击“新建”按钮创建安全域。如果希望安全域内的接口之间可以通信,请勾选“允许接口间互相访问”复选框。在“接口成员”区域可以选择加入到该安全域的接口,如图 6-12 所示。




图 6-12　创建安全域

### 5. 配置网关

进入“基本配置”页面, 如图 6-13 所示。

单击“新建”配置默认网关。如果希望安全域内的接口之间可以通信,请勾选“允许接口间互相访问”复选框。在“接口成员”区域可以选择加入到该安全域的接口,如图 6-14 所示。




图 6-13　配置网关




图 6-14　选择加入到安全域接口

## 6. 配置路由

进入“路由表”页面，可以查看当前 USG 的路由表。之前在“基本配置”页面上添加的网关也将作为默认路由出现在路由表中，如图 6-15 所示。

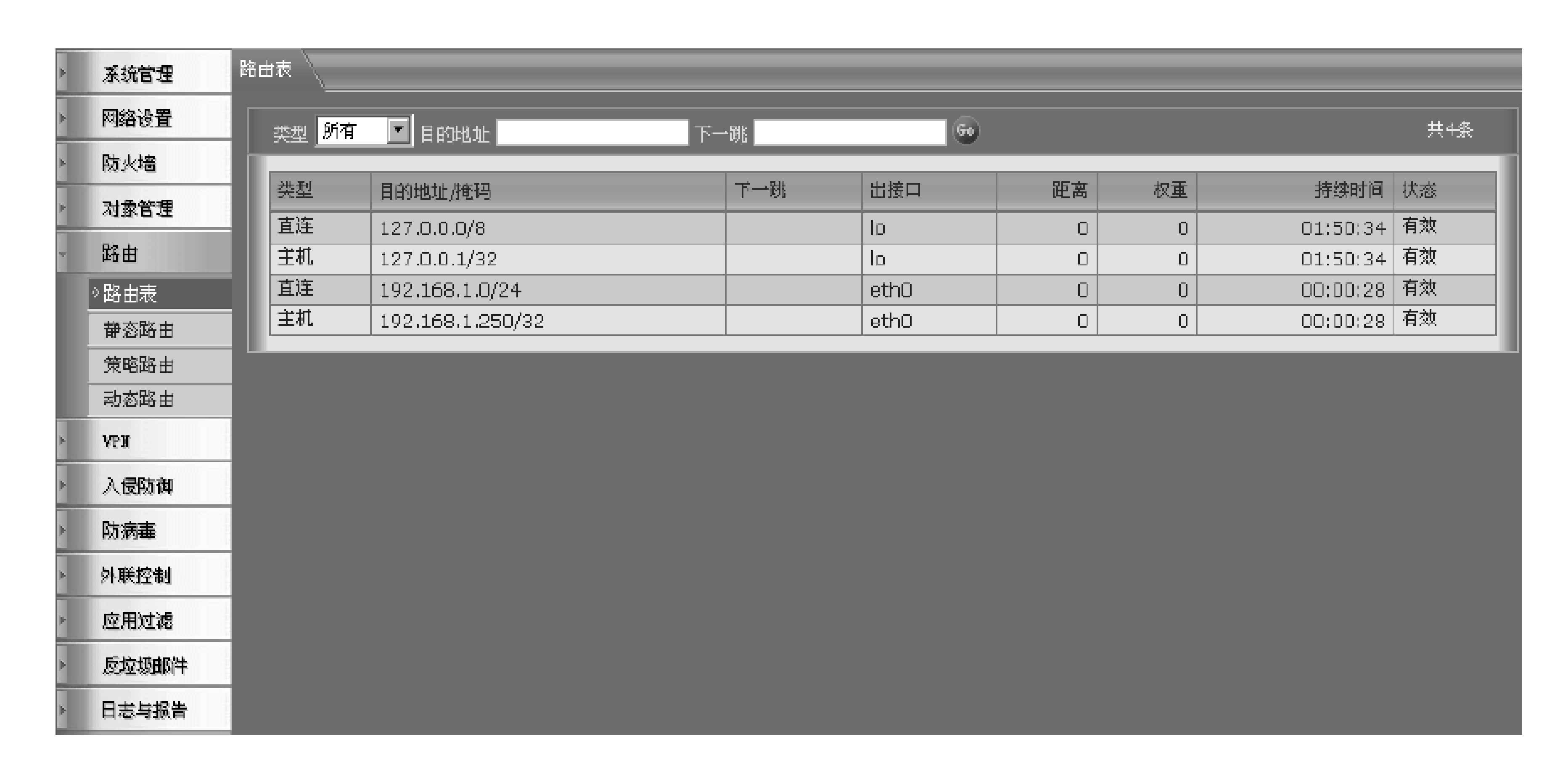



图 6-15　配置路由信息

进入“静态路由”页面，单击“新建”按钮添加静态路由，如图 6-16 和图 6-17 所示。




图 6-16　添加静态路由(1)




图 6-17　添加静态路由(2)

### 7. 重启 USG

进入“维护”页面，可以选择重启系统或者恢复出厂设置，恢复出厂设置需要重新启动，如图 6-18 所示。




图 6-18　恢复出厂设置

## 6.2 用户权限管理

### 【实验名称】

用户权限管理。

### 【实验目的】

为 USG 创建新管理用户，并为不同的管理用户分配不同的管理权限。

### 【背景描述】

某企业为了提高网络的安全性，购买了一台 RG-USG 统一安全网关。现在为了提高对设备管理的安全性，需要由 3 个不同的管理员来管理 USG，但是这些管理员要拥有不同的管理权限。

在 3 个管理员中，第一个管理员只能够对 USG 采取只读的操作，例如查看配置；第二个管理员不仅能够对 USG 进行读取操作，而且还需要对 USG 进行配置，例如配置安全策略，但不能对 USG 进行升级、重启等操作；第三个管理员拥有最高的管理权限，不仅可以读取配置、配置策略，还能够对设备进行升级、重启、配置管理员等操作。

### 【需求分析】

为了实现多个不同权限的管理员对 USG 进行管理，需要在 USG 上创建多个管理用户，并且赋予他们不同的管理权限。

### 【实验拓扑】

如图 6-19 所示的网络拓扑，是企业为了提高网络的安全，购买的一台 RG-USG 统一安全网关。现在为了提高对设备管理的安全性，需要由 3 个不同的管理员来管理 USG，管理员要拥有不同的管理权限，现在需要登录到 USG 并对其进行配置，以实现网络安全防范功能。

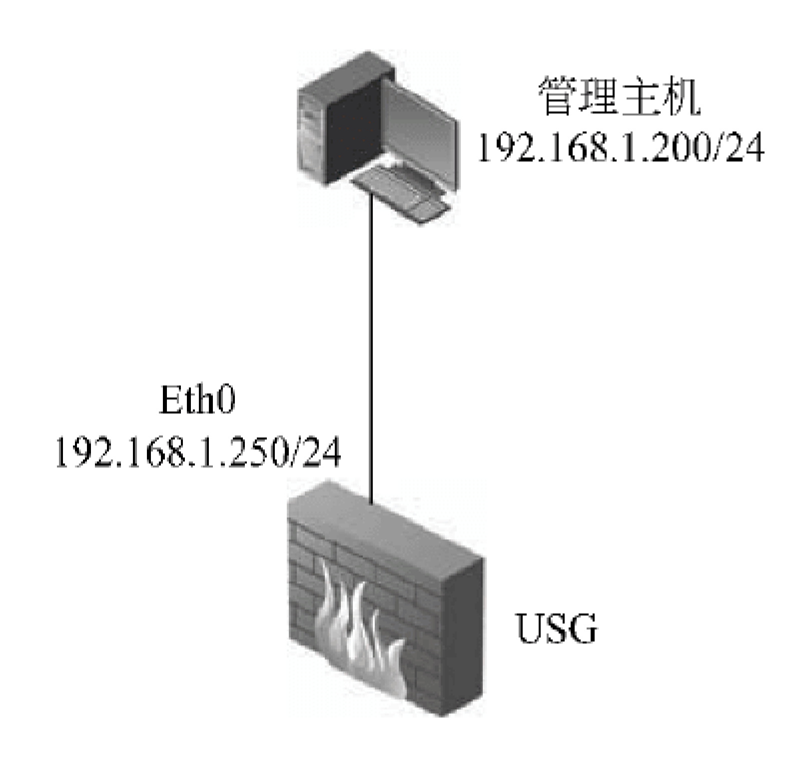



图 6-19　USG 用户权限管理网络拓扑图

### 【实验设备】

USG　1 台
PC　1 台

### 【预备知识】

- 网络基础知识。
- USG 操作基础知识。

## 【实验原理】

USG 支持多管理员,并且可以为不同的管理员赋予不同的管理权限,为 USG 提供了安全的管理机制。

## 【实验步骤】

### 1. 使用默认的管理员账号登录 USG

在默认出厂配置中,USG 的 Eth0 接口预先配置了 IP 地址 192.168.1.250/24,所以在本实验中使用地址为相同子网的管理主机 192.168.1.200/24 连接到 Eth0 接口对 USG 进行管理,如图 6-20 所示。




图 6-20　使用默认的管理员账号登录 USG

USG 使用 HTTPS 对管理流量进行加密。在浏览器的地址栏中输入 https://192.168.1.250,浏览器将提示是否接受 USG 的证书,单击“是”按钮。

接受证书后,将进入到 USG 登录界面,默认的用户名为 admin,密码为 ruijie.USG,如图 6-21 所示。

单击“登录”按钮后,进入 USG Web 管理界面。进入“管理员”页面,这里可以看到系统默认的管理员为 admin,并且绑定的访问权限列表为 admin。admin 访问权限列表也是系统预定义的,该权限列表具有最高等级的管理权限,如图 6-22 所示。

### 2 配置具有只读权限的管理员

进入“管理员”页面,选择“管理员权限表”选项卡,可以看到系统预定义的权限列表 admin。admin 权限列表具有所有的管理权限,如图 6-23 和图 6-24 所示。

单击“新建”按钮后创建权限列表,并为该权限列表定义只读权限,如图 6-25 所示。




图 6-21　进入到 USG 登录界面




图 6-22　使用系统默认的管理员权限




图 6-23　配置具有只读权限的管理员(1)




图 6-24　配置具有只读权限的管理员(2)

新建管理员权限表

| | |
|---|---|
| 名称 | read-only |
| 描述 | |

| 访问控制 | ☑ 全部允许读 | ☐ 全部允许写 |
|---|---|---|
| 系统配置 | ☑ 读 | ☐ 写 |
| 安全策略 | ☑ 读 | ☐ 写 |
| 配置管理员 | ☑ 读 | ☐ 写 |
| 配置认证用户 | ☑ 读 | ☐ 写 |
| 升级管理 | ☑ 读 | ☐ 写 |
| 日志与报告 | ☑ 读 | ☐ 写 |
| 系统重启 | ☐ 读 | ☐ 写 |

提交　取消

图 6-25　创建权限列表

进入“管理员”页面,单击“新建”按钮添加管理员账号,并为该管理员配置用户名、密码和访问权限。在访问权限中选择刚刚创建的 read-only 权限列表,如图 6-26 所示。




图 6-26　添加管理员账号

注销当前用户,重新使用 admin_view 用户登录,如图 6-27 所示。




图 6-27　创建一个安全策略

进入“安全策略”页面，单击“新建”按钮创建一个安全策略。

单击“提交”按钮后，系统提示当前用户没有权限配置策略，所以该用户只能对 USG 进行读取操作，如图 6-28 所示。

注销当前用户，重新使用默认的 admin 用户登录。




图 6-28　当前用户没有权限配置策略

### 3. 配置具有配置权限的管理员

进入“管理员”页面，选择“管理员权限表”选项卡。

单击“新建”按钮后创建权限列表，并为该权限列表定义读取和配置权限，如图 6-29 所示。

新建管理员权限表

名称　config

描述

| 访问控制 | ☑ 全部允许读 | ☐ 全部允许写 |
|---|---|---|
| 系统配置 | ☑ 读 | ☑ 写 |
| 安全策略 | ☑ 读 | ☑ 写 |
| 配置管理员 | ☑ 读 | ☐ 写 |
| 配置认证用户 | ☑ 读 | ☑ 写 |
| 升级管理 | ☑ 读 | ☐ 写 |
| 日志与报告 | ☑ 读 | ☐ 写 |
| 系统重启 | ☐ 读 | ☐ 写 |

提交　取消

图 6-29　配置具有配置权限的管理员

进入“管理员”页面，单击“新建”按钮添加管理员账号，并为该管理员配置用户名、密码和访问权限。在访问权限中选择刚刚创建的 config 权限列表，如图 6-30 所示。




图 6-30　添加管理员账号访问权限

注销当前用户，重新使用 admin_config 用户登录，如图 6-31 所示。




图 6-31　创建安全策略

进入“安全策略”页面，单击“新建”按钮创建一个安全策略。

单击“提交”按钮后，策略配置成功，说明该用户具有配置的权限，如图 6-32 所示。

进入“维护”页面，选择“重启系统”选项卡，这时系统会提示该用户没有权限，因为之前没有给该用户分配重启系统的权限，如图 6-33 所示。

注销当前用户，重新使用默认的 admin 用户登录。

## 4. 配置具有所有权限的管理员

进入“管理员”页面，选择“管理员权限表”选项卡。

单击“新建”按钮后创建权限列表，并为该权限列表定义所有权限，如图 6-34 所示。

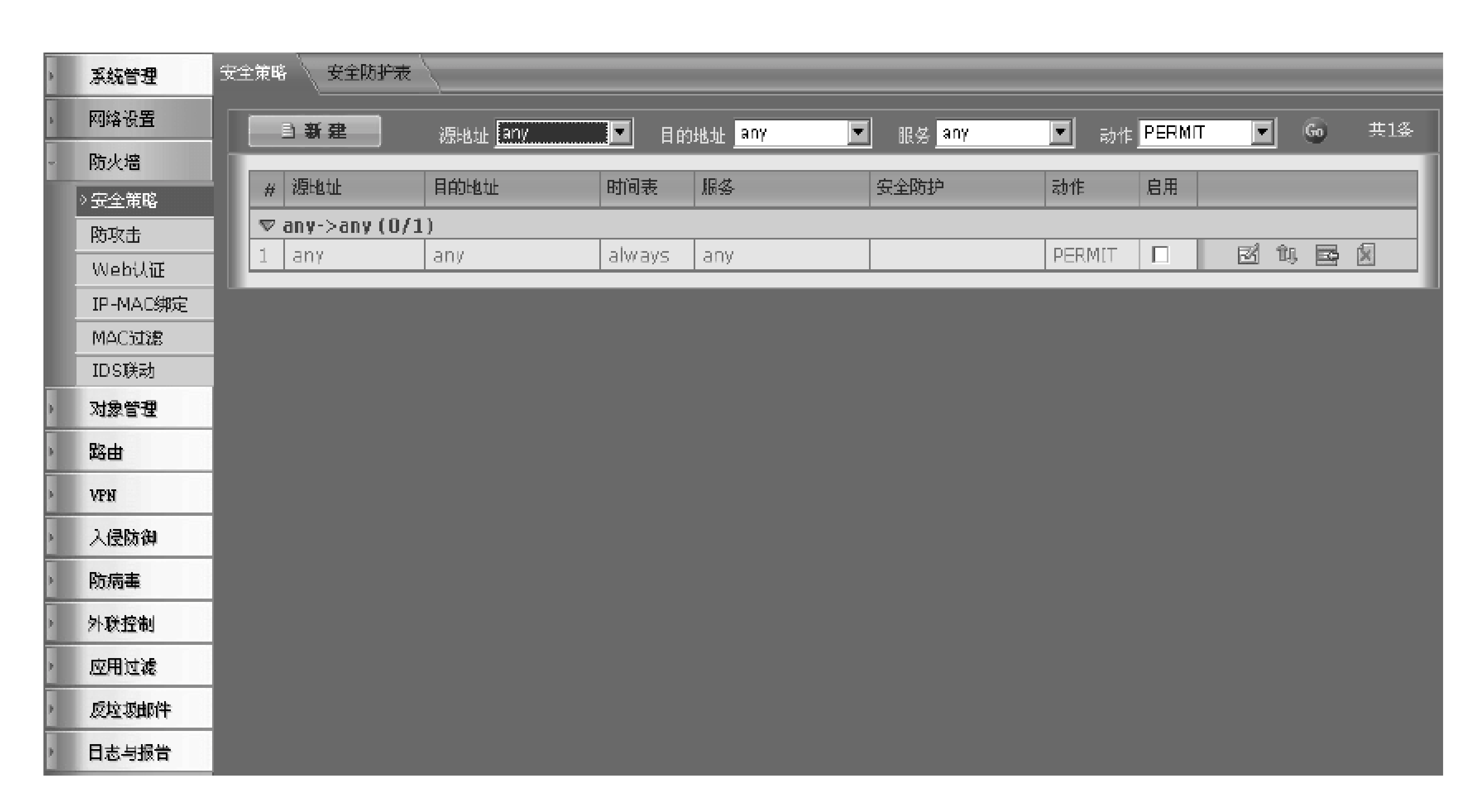



图 6-32　配置用户具有的权限




图 6-33　用户没有分配重启系统的权限




图 6-34　配置具有所有权限的管理员

进入“管理员”页面，单击“新建”按钮添加管理员账号，并为该管理员配置用户名、密码和访问权限。在访问权限中选择刚刚创建的 super_admin 权限列表，如图 6-35 所示。




图 6-35　添加管理员账号

注销当前用户，重新使用 admin_super 用户登录，如图 6-36 所示。




图 6-36　创建安全策略

进入“安全策略”页面，单击“新建”按钮创建一个安全策略。

单击“提交”按钮后，策略配置成功，说明该用户具有配置的权限，如图 6-37 所示。

进入“维护”页面，选择“重启系统”选项卡，单击“提交”按钮后可以重启系统，说明该用户具有最高的权限，如图 6-38 所示。

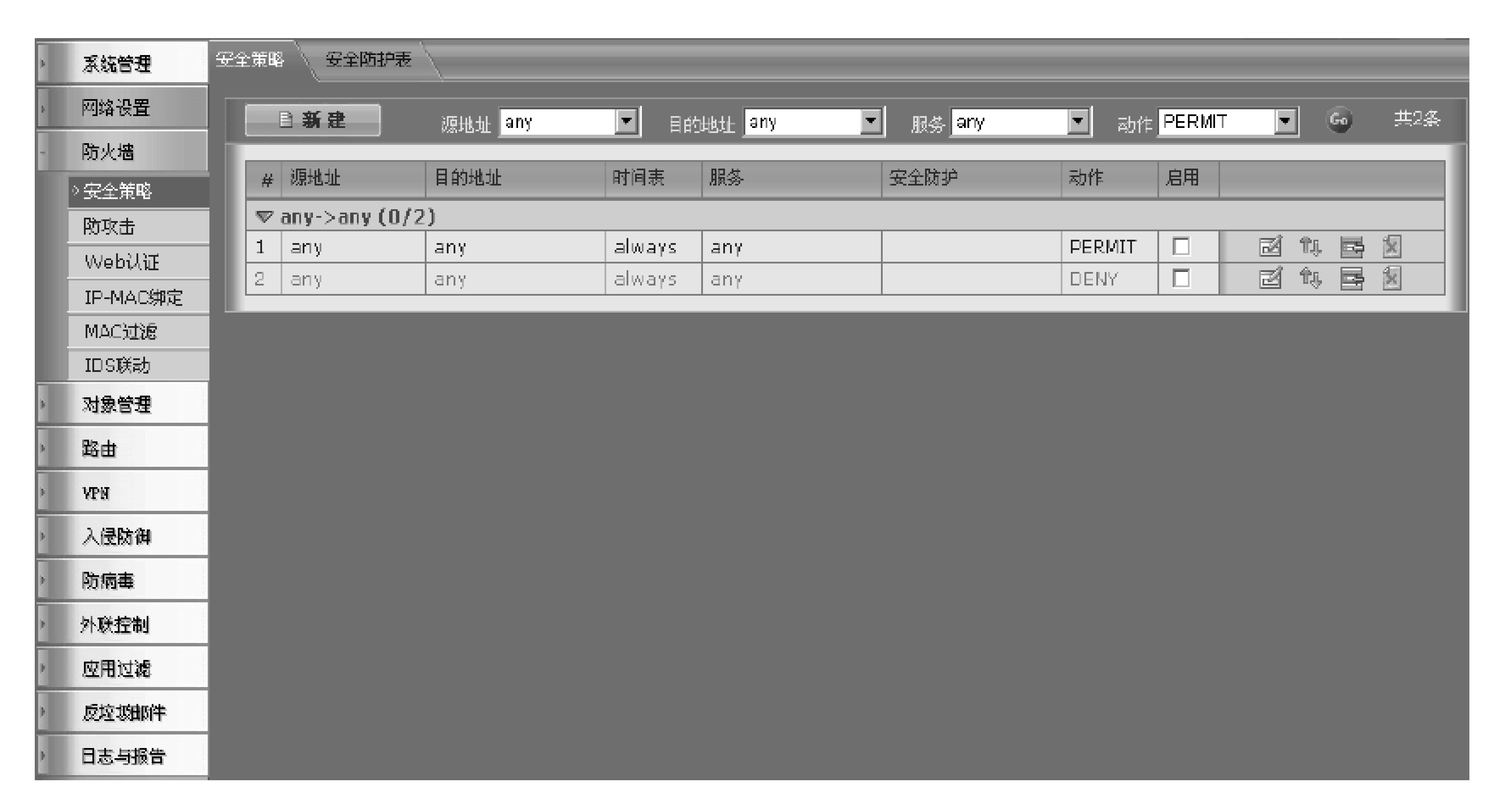



图 6-37　配置用户具有的权限




图 6-38　配置用户具有重启系统的权限

# 6.3　使用统一安全网关实现访问控制

## 【实验名称】

使用统一安全网关实现访问控制。

## 【实验目的】

利用 USG(统一安全网关)的安全策略和 NAT 功能实现安全的访问控制。

## 【背景描述】

某企业网络的出口使用一台 USG(统一安全网关)作为接入 Internet 的设备,并且内部网络使用私有 IP 地址(RFC 1918)。现在需要使内部网络中的主机访问 Internet 资源,并且还需要进行访问控制,只允许必要的流量通过 USG。

企业内部网络使用的私有地址段为 10.1.1.0/24、10.1.2.0/24 和 10.1.3.0/24。公司领导使用的子网为 10.1.1.0/24,设计部使用的子网为 10.1.2.0/24,其他员工使用的子网为 10.1.3.0/24。并且公司在公网上有一台 IP 地址为 200.1.1.1 的外部 FTP 服务器。

现在需要在 USG 上进行访问控制,使公司领导的主机可以在任何时间访问 Internet 中的 Web 服务器和 FTP 服务器,并能够使用邮件客户端(SMTP/POP3)收发邮件;设计部的主机只能在上班时间(每周一至周五的 9:00～18:00)访问 Internet 中的 Web 服务器和公司的外部 FTP 服务器;其他员工的主机只能在上班时间访问公司的外部 FTP 服务器。

## 【需求分析】

企业网络需要允许使用私有编址的内部网络能够访问 Internet,并且对内部网络访问 Internet 的流量进行限制,USG 的安全策略和 NAT 功能可以同时满足这两个需求。

## 【实验拓扑】

如图 6-39 所示的网络拓扑,是企业为了提高网络的安全,购买的一台 RG-USG 统一安全网关。

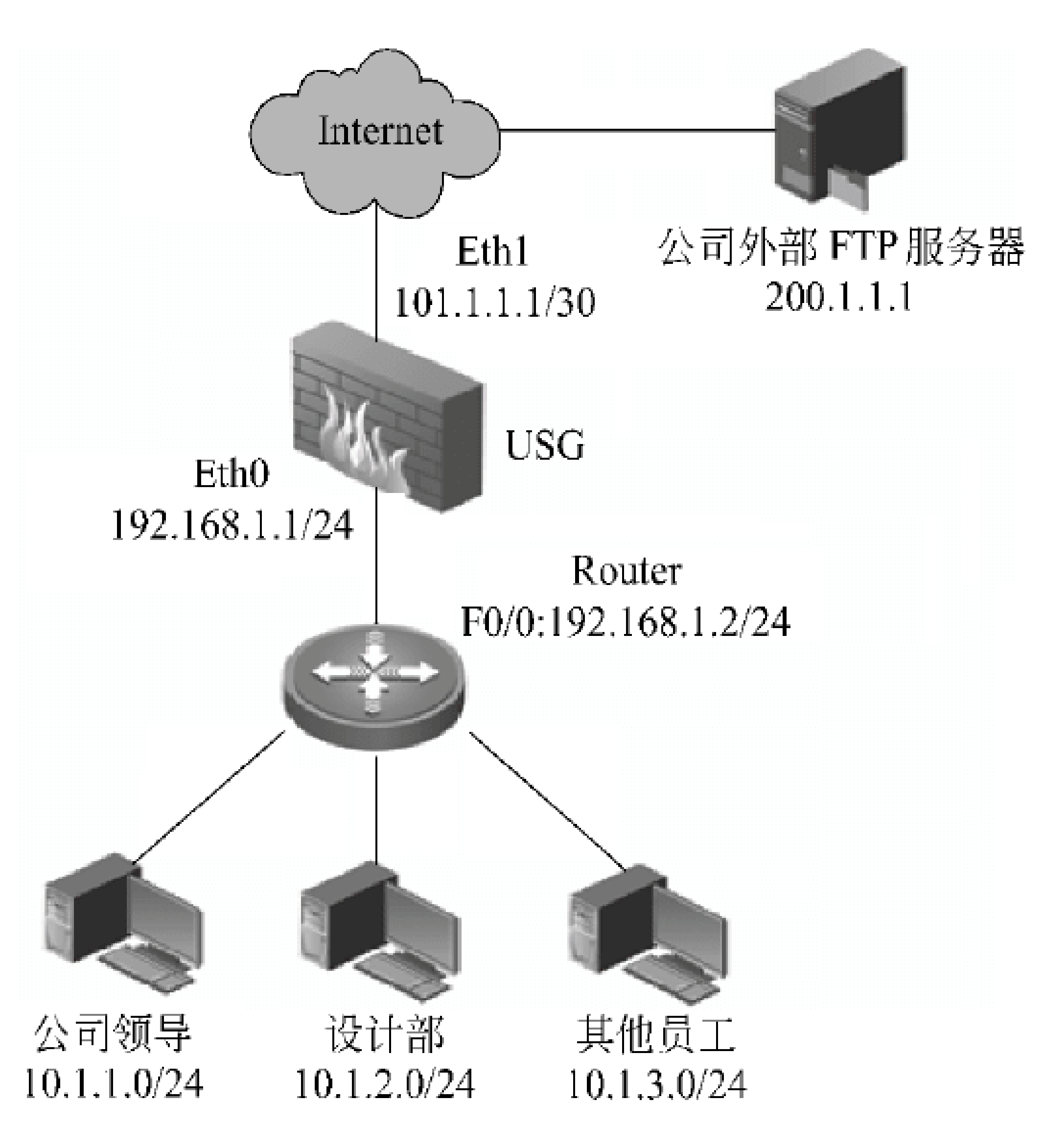



图 6-39　使用统一安全网关实现访问控制网络拓扑图

利用 USG(统一安全网关)的安全策略和 NAT 功能实现安全的访问控制,使私有编址的内部网络能够访问 Internet,并且对内部网络访问 Internet 的流量进行限制,以实现

网络的安全防范功能。

## 【实验设备】

USG 连接到 Internet 的链路

| | |
|---|---|
| USG | 1 台 |
| 路由器 | 1 台 |
| PC | 3 台 |
| FTP 服务器 | 1 台 |

## 【预备知识】

- 网络基础知识。
- USG 基础知识。

## 【实验原理】

实现访问控制是 USG 的基本功能，USG 的安全策略（包过滤规则）可以根据数据包的源 IP 地址、目的 IP 地址、服务（端口号）等对通过 USG 的报文进行检测。并且 USG 的 NAT 功能可以对通过 USG 的报文进行转换，使私有编址的主机可以访问 Internet。

## 【实验步骤】

### 1. 配置 USG 接口的 IP 地址

进入 USG 的配置页面，即“接口”界面，如图 6-40 所示。




图 6-40　进入 USG 的配置页面

单击 eth0 接口的“编辑”图标，为 eth0 接口配置 IP 地址及子网掩码，如图 6-41 所示。

单击 eth1 接口的“编辑”图标，为 eth1 接口配置 IP 地址及子网掩码，如图 6-42 所示。

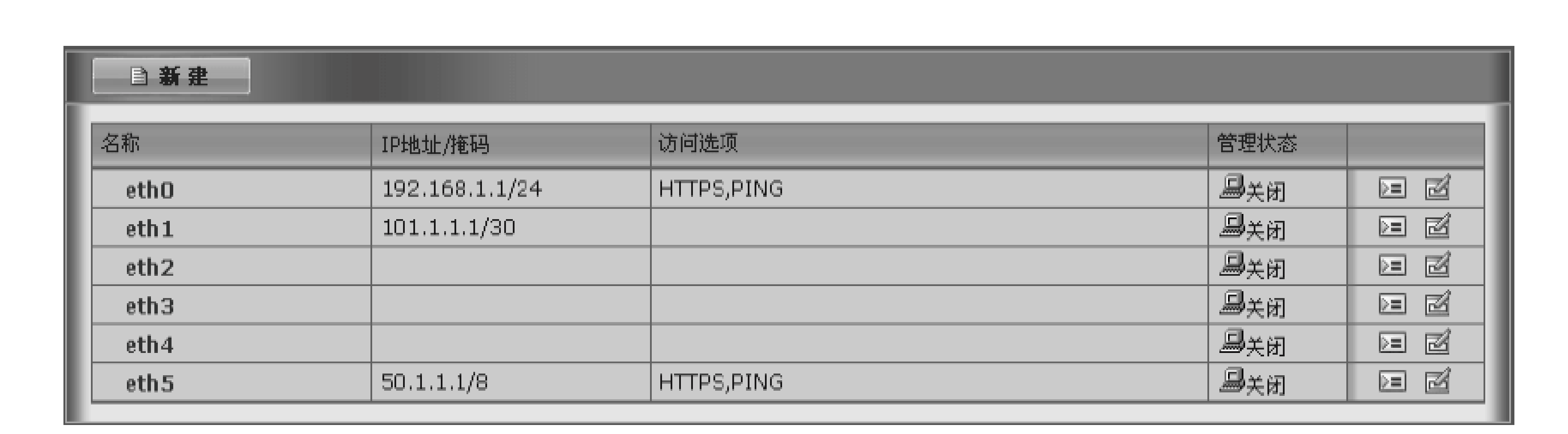
接口配置 IP 地址后的状态如图 6-43 所示。




图 6-41　为 eth0 接口配置 IP 地址




图 6-42　为 eth1 接口配置 IP 地址



新建

| 名称 | IP地址/掩码 | 访问选项 | 管理状态 | |
|---|---|---|---|---|
| eth0 | 192.168.1.1/24 | HTTPS,PING | 关闭 | |
| eth1 | 101.1.1.1/30 | | 关闭 | |
| eth2 | | | 关闭 | |
| eth3 | | | 关闭 | |
| eth4 | | | 关闭 | |
| eth5 | 50.1.1.1/8 | HTTPS,PING | 关闭 | |

图 6-43　接口 IP 地址信息

## 2 配置内部子网的地址对象

进入 USG 的配置页面，即“地址对象”页面。可以看到系统预定义了一个名为 any 的地址对象，它包括所有的地址 0.0.0.0/0，如图 6-44 所示。

单击“新建”按钮创建地址对象，该地址对象包括公司领导主机的子网 10.1.1.0/24，如图 6-45 所示。

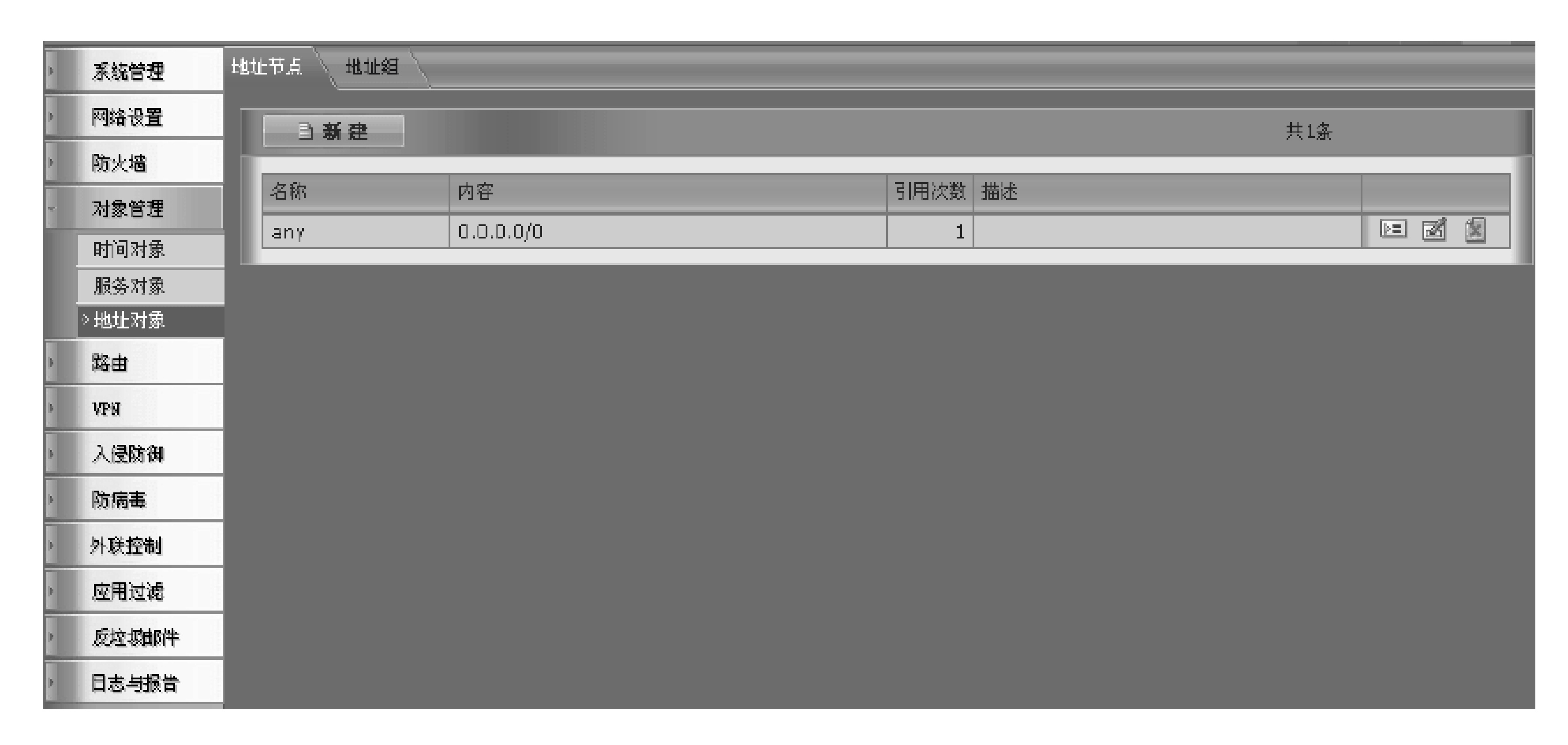



图 6-44　配置内部子网的地址

新建地址节点
名称　manager
描述
地址节点
主机
子网　10.1.1.0/24
范围
10.1.1.0/24
提交　取消

图 6-45　创建地址对象(1)

创建包括设计部子网 10.1.2.0/24 的地址对象，如图 6-46 所示。



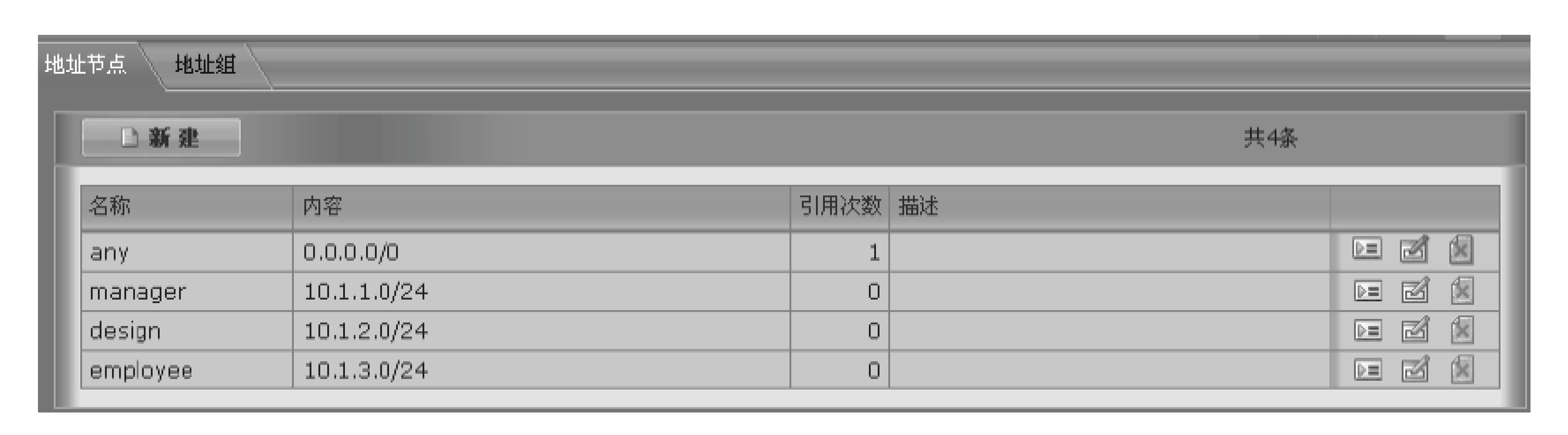

图 6-46　创建地址对象(2)

创建包括其他员工子网 10.1.3.0/24 的地址对象，如图 6-47 所示。

创建完地址对象后的地址对象列表如图 6-48 所示。




图 6-47　创建地址对象(3)




| 名称 | 内容 | 引用次数 | 描述 |
|---|---|---|---|
| any | 0.0.0.0/0 | 1 | |
| manager | 10.1.1.0/24 | 0 | |
| design | 10.1.2.0/24 | 0 | |
| employee | 10.1.3.0/24 | 0 | |

图 6-48　地址对象列表

## 3. 配置地址组

进入 USG 配置页面，即“地址对象”页面，选择“地址组”选项卡，如图 6-49 所示。




图 6-49　配置地址组

单击“新建”按钮创建地址组。地址组实际上是地址对象的集合，一个地址组可以包括多个地址对象或者嵌套多个地址组，如图 6-50 和图 6-51 所示。

## 4. 配置 NAT

进入 USG 的配置页面，即 NAT 页面。单击“新建”按钮创建 NAT 规则，如图 6-52 所示。




图 6-50　创建地址组(1)




图 6-51　创建地址组(2)




图 6-52　创建 NAT 规则(1)

在 NAT 规则中的源地址选择之前先创建 inside 地址组，目标地址使用 any 地址对象，服务使用 any 服务对象，出接口为连接 Internet 的 eth1 接口，转换后源地址为“出接口地址”，即 eth1 接口的地址，如图 6-53 所示。




图 6-53　创建 NAT 规则(2)

### 5. 配置针对公司领导主机的安全策略

创建包括 HTTP、FTP、DNS、SMTP、POP3 服务的服务组。进入 USG 的配置页面，

即“服务对象”页面，选择“服务组”选项卡，如图 6-54 所示。




图 6-54　进入 USG 的配置页面

单击“新建”按钮创建服务组。服务组实际上是服务对象的集合，一个服务组可以包括多个服务对象或者嵌套多个服务组，这与地址组的概念相同，如图 6-55 所示。




图 6-55　创建基本服务的服务组

配置安全策略，进入 USG 配置页面，即“安全策略”页面，如图 6-56 所示。

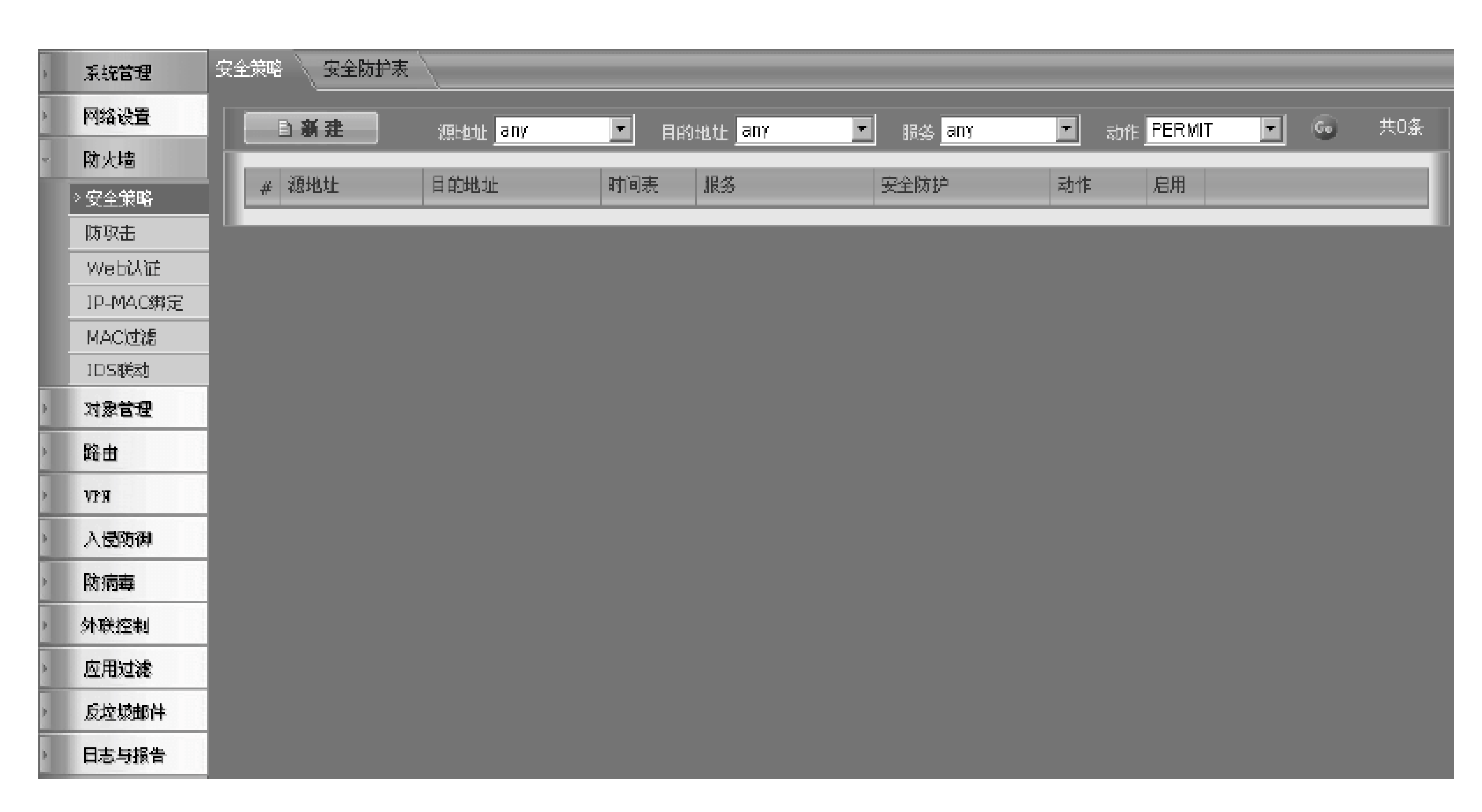



图 6-56　配置安全策略

单击“新建”按钮创建安全策略。安全策略中源接口为 eth0 接口；源地址为 manager 地址对象；目的接口为 eth1 接口；目的地址为 any 地址对象；服务为 manager 服务组；时间表为 always 地址对象，代表任何时间；动作为 PERMIT 允许，如图 6-57 所示。




图 6-57　创建安全策略

创建完安全策略后，需要选择“启用”选项来使该规则生效，如图 6-58 所示。




图 6-58　启用安全规则

## 6. 配置针对设计部主机的安全策略

创建包括 HTTP、FTP、DNS 服务的服务组。进入 USG 的配置页面，即“服务对象”页面，选择“服务组”选项卡，单击“新建”按钮，打开如图 6-59 所示对话框。




图 6-59　创建服务组

创建包括公司外部 FTP 服务器的地址对象。进入 USG 的配置页面，即“地址对象”页面，单击“新建”按钮添加地址对象，启动如图 6-60 所示对话框。

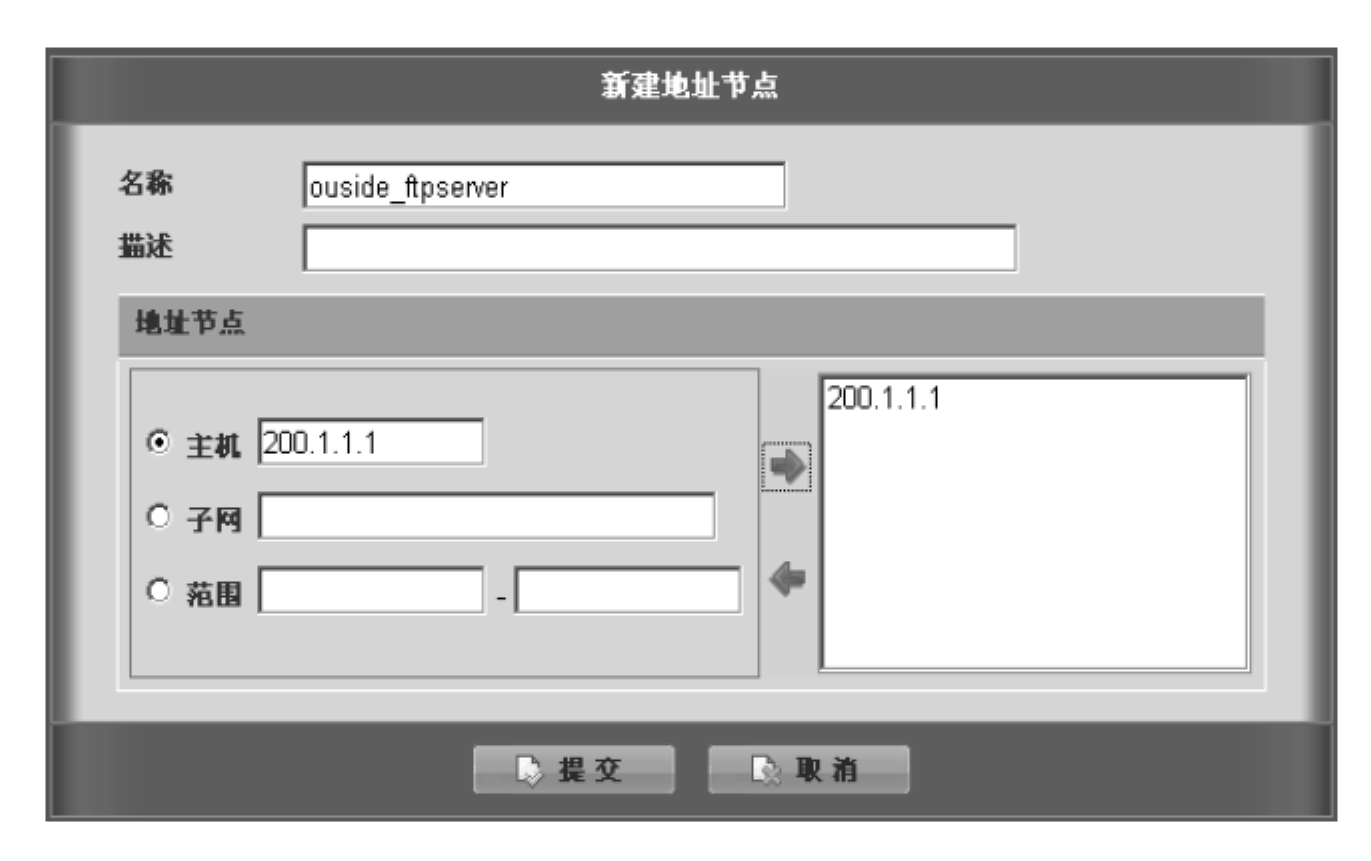



图 6-60　添加地址对象

创建包括上班时间的时间对象。进入 USG 配置页面，即“时间对象”页面，选择“周期时间”选项卡，如图 6-61 所示。




图 6-61　创建上班时间对象

单击“新建”按钮，创建时间对象。为时间对象输入名称，如图 6-62 所示。




图 6-62　为时间对象输入名称

单击之前页面上的“新增”按钮来增加时间段。选择星期选项，并选择开始时间和结束时间，如图6-63所示。




图6-63　新增时间段

单击“提交”按钮，如图6-64和图6-65所示。

图6-64　新增时间周期

图6-65　浏览新增时间周期

配置允许设计部访问Web服务器的安全策略，进入USG配置页面，即“安全策略”页面。

单击“新建”按钮创建安全策略。安全策略中源接口为eth0接口；源地址为design地址对象；目的接口为eth1接口；目的地址为any地址对象；服务为design服务组；时间表为之前创建的work-time地址对象，代表上班时间；动作为PERMIT允许，如图6-66所示。

配置允许设计部访问公司外部FTP服务器的安全策略，进入USG配置页面，即“安全策略”页面。

图 6-66　创建安全策略(1)

单击“新建”按钮创建安全策略。安全策略中源接口为 eth0 接口;源地址为 design 地址对象;目的接口为 eth1 接口;目的地址为之前创建的 outside_ftpserver 地址对象;服务为 ftp 服务对象;时间表为 work-time 地址对象,代表上班时间;动作为 PERMIT 允许,如图 6-67 所示。




图 6-67　创建安全策略(2)

创建完安全策略后,需要选择“启用”选项来使该规则生效,如图 6-68 所示。

### 7. 配置针对其他员工主机的安全策略

配置允许其他员工访问公司外部 FTP 服务器的安全策略,进入 USG 配置页面,即“安全策略”页面。



| # | 源地址 | 目的地址 | 时间表 | 服务 | 安全防护 | 动作 | 启用 |
|---|---|---|---|---|---|---|---|
| eth0->eth1 (3/3) | | | | | | | |
| 1 | manager | any | always | manager | | PERMIT | ☑ |
| 2 | design | any | work-time | design | | PERMIT | ☑ |
| 3 | design | ouside_ftpserver | work-time | ftp | | PERMIT | ☑ |

图 6-68　启用创建的安全策略(1)

单击“新建”按钮创建安全策略。安全策略中源接口为 eth0 接口;源地址为 employee 地址对象;目的接口为 eth1 接口;目的地址为之前创建的 outside_ftpserver 地址对象;服务为 ftp 服务对象;时间表为 work-time 地址对象,代表上班时间;动作为 PERMIT 允许,如图 6-69 所示。




图 6-69　创建安全策略

创建完安全策略后,需要选择“启用”选项来使该规则生效,如图 6-70 所示。



| # | 源地址 | 目的地址 | 时间表 | 服务 | 安全防护 | 动作 | 启用 |
|---|---|---|---|---|---|---|---|
| eth0->eth1 (4/4) | | | | | | | |
| 1 | manager | any | always | manager | | PERMIT | ☑ |
| 2 | design | any | work-time | design | | PERMIT | ☑ |
| 3 | design | ouside_ftpserver | work-time | ftp | | PERMIT | ☑ |
| 4 | employee | ouside_ftpserver | work-time | ftp | | PERMIT | ☑ |

图 6-70　启用创建的安全策略(2)

## 8. 验证测试

- 公司领导的主机可以访问 Internet 中的 Web 服务器和 FTP 服务器,并能够使用邮件客户端(SMTP/POP3)收发邮件。

- 设计部的主机可以访问 Internet 中的 Web 服务器和公司的外部 FTP 服务器。
- 其他员工的主机只能访问公司的外部 FTP 服务器。

### 【注意事项】

- USG 的安全策略是按照顺序进行匹配的，如果数据流匹配到某条规则后，将不再进行后续规则的匹配。
- 在默认情况下，USG 拒绝所有没有明确允许的数据流通过，并且不对其进行地址转换。
- 在本实验中没有给出 USG 路由的配置，需要根据实际网络情况在 USG 上配置访问 Internet(通常是默认路由)和内部网络的路由。
- 本实验没有给出内部网络中路由器的配置，为了实现网络的互通，需要在路由器上配置地址和相关路由信息。

## 6.4　使用统一安全网关防止 DoS 攻击

### 【实验名称】

使用统一安全网关防止 DoS 攻击。

### 【实验目的】

利用 USG(统一安全网关)的防攻击功能防止 SYN Flood 攻击。

### 【背景描述】

某公司使用 USG 作为网络出口设备连接 Internet，并且公司内部有一台对外提供服务的 FTP 服务器。最近网络管理员发现在 Internet 中有人向 FTP 服务器发起 SYN Flood 攻击，造成 FTP 上存在大量的半开放连接，消耗了服务器的系统资源。

### 【需求分析】

要防止来自外部网络的 DoS 攻击，可以使用 USG 的防攻击功能。

### 【实验拓扑】

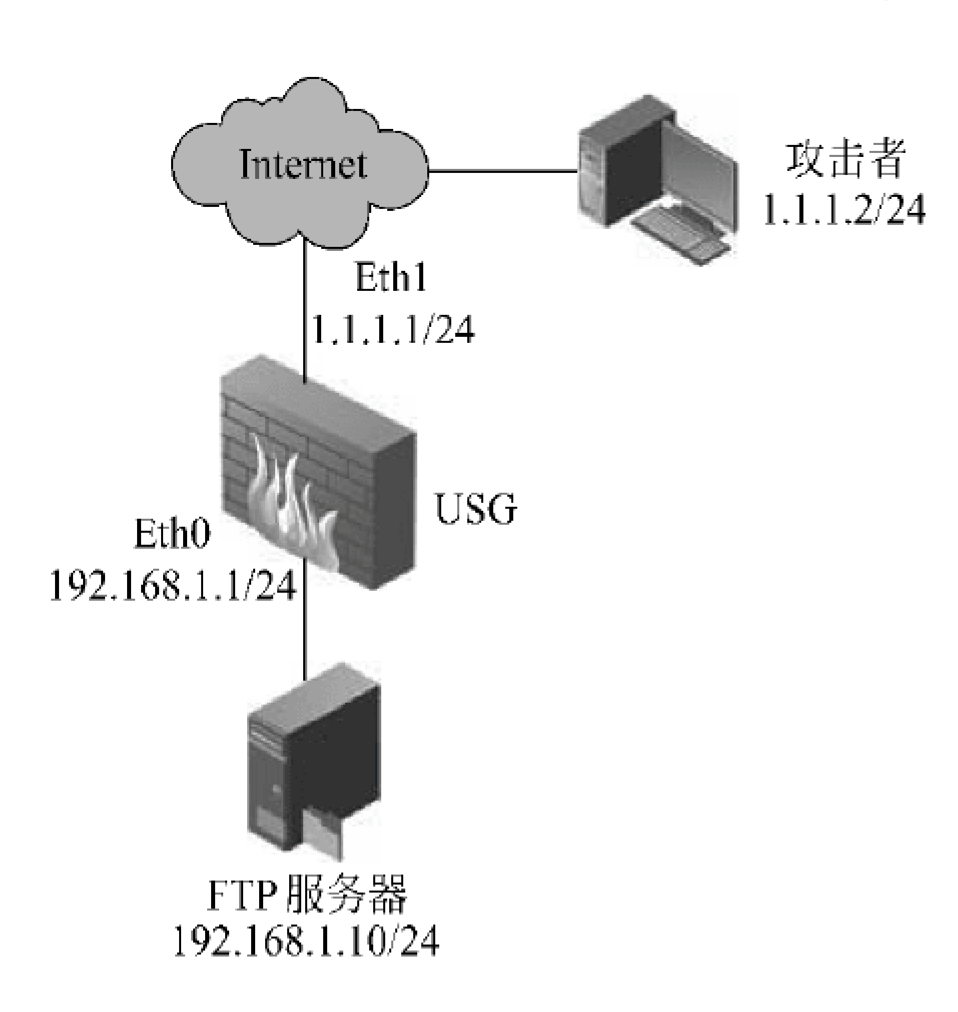


图 6-71　统一安全网关防止 DoS 攻击网络拓扑图

如图 6-71 所示的网络拓扑，是企业网络管理员发现在 Internet 中有人向 FTP 服务器发起 SYN Flood 攻击，造成 FTP 上存在大量的

半开放连接，消耗了服务器的系统资源。为了提高网络的安全，购买了一台 RG-USG 统一安全网关，并对其进行基本配置，使用统一安全网关防止 DoS 攻击，以实现网络的安全防范功能。

## 【实验设备】

USG　1 台
PC　　2 台（一台作为 FTP 服务器；另一台模拟外部网络的攻击者）
FTP 服务器软件程序
SYN Flood 攻击软件程序

## 【预备知识】

- 网络基础知识。
- USG 操作基础知识。
- DoS 攻击原理。

## 【实验原理】

SYN Flood 是一种常见的 DoS 攻击，这种攻击通过使用伪造的源 IP 地址，向目标主机（被攻击端）发送大量的 TCP SYN 报文。目标主机接收到 SYN 报文后，会向伪造的源地址回应 TCP SYN_ACK 报文以等待发送端的 ACK 报文来建立连接。但是由于发送端的地址是伪造的，所以被攻击端永远不会收到合法的 ACK 报文，这将造成被攻击端建立大量的半开放连接，消耗大量的系统资源，导致不能提供正常的服务。

USG 的防攻击功能可以对 SYN Flood/TCP Flood 攻击进行检测，阻止大量的 TCP SYN 报文到达被攻击端，从而保护内部主机的资源。

## 【实验步骤】

### 1. 配置 USG接口的 IP地址

如图 6-72 所示，进入 USG 的配置页面，即“接口”页面。




图 6-72　进入 USG 的配置页面

单击 eth0 接口的“编辑”图标，为 eth0 接口配置 IP 地址及子网掩码，如图 6-73 所示。




图 6-73　为 eth0 接口配置 IP 地址

单击 eth1 接口的“编辑”图标，为 eth1 接口配置 IP 地址及子网掩码，如图 6-74 所示。




图 6-74　为 eth1 接口配置 IP 地址

接口配置 IP 地址后的状态如图 6-75 所示。

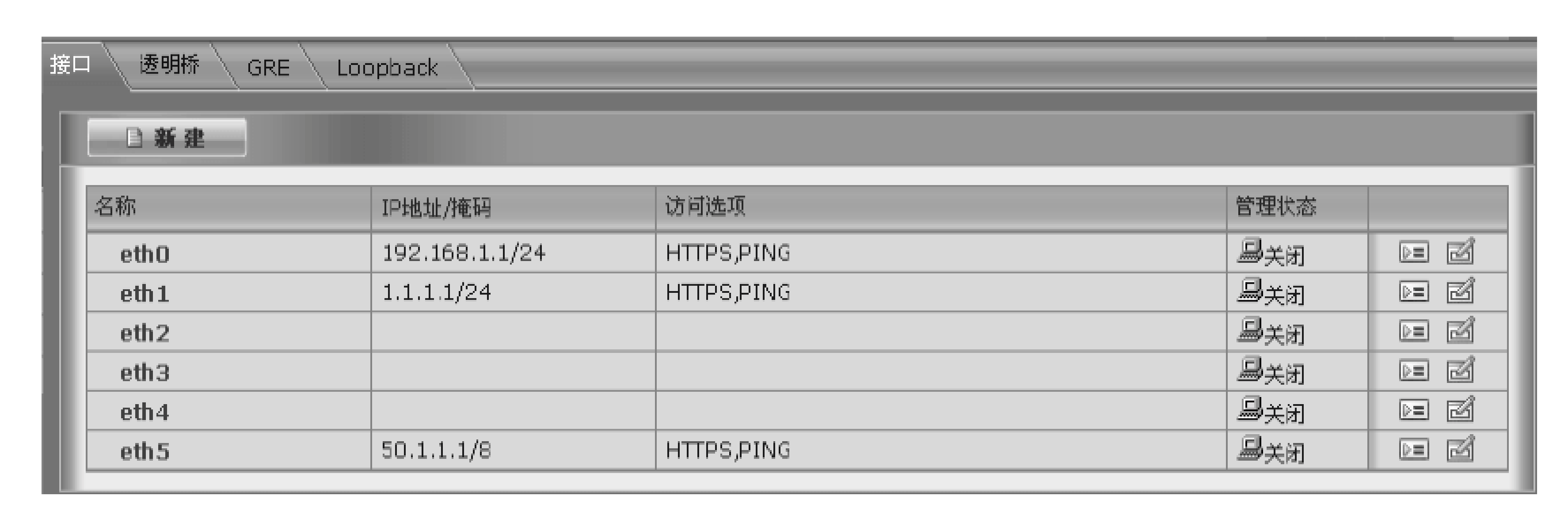



图 6-75　接口配置 IP 地址

### 2 配置静态 NAT 转换

为了使 Internet 中的用户可以访问内部的 FTP 服务器，需要在 USG 上配置静态 NAT 转换，将 FTP 服务器发布到 Internet 中。

进入 USG 配置页面，即 NAT 页面，选择“静态地址转换”单选按钮，如图 6-76 所示。




图 6-76　在 USG 上配置静态 NAT 转换

单击“新建”按钮创建静态地址转换规则。规则中的“外部地址”为 FTP 服务器对外发布的地址；“内部地址”为 FTP 服务器实际的内部地址；“外部接口”为连接 Internet 的 eth1 接口，如图 6-77 所示。




图 6-77　创建静态地址转换规则

### 3 配置安全策略

首先进入 USG 配置页面，即“地址对象”页面。配置包含内部 FTP 服务器的地址对象，如图 6-78 所示。

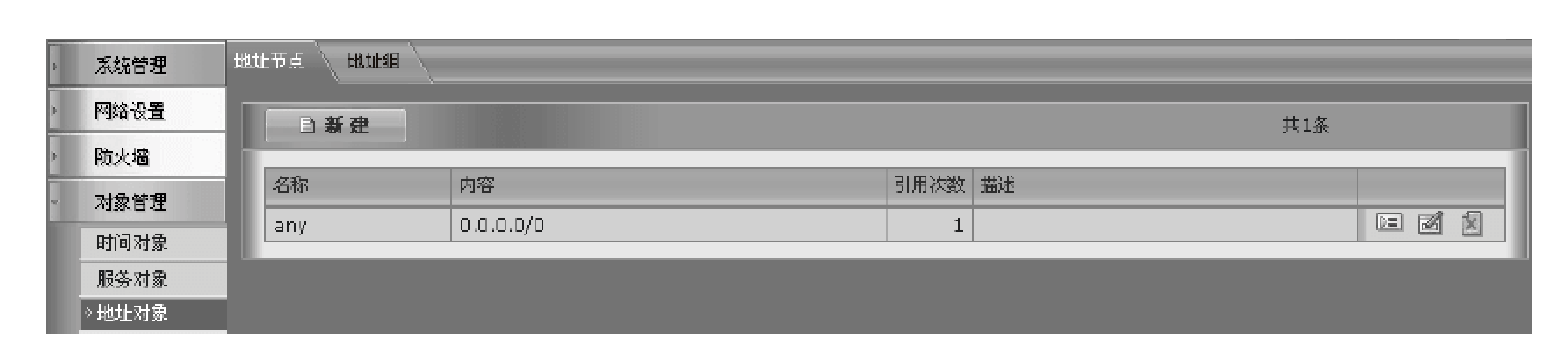



图 6-78　配置内部 FTP 服务器地址对象

单击“新建”按钮创建地址对象，地址为 FTP 服务器的内部地址 192.168.1.10，如图 6-79 所示。

进入 USG 配置页面，即“安全策略”页面，配置允许外部访问 FTP 服务器的安全策略。

单击“新建”按钮创建安全策略。安全策略中源接口为 eth1 接口；源地址为 any 地址




图 6-79　创建地址对象

对象;目的接口为 eth0 接口;目的地址为 FTPSERVER 地址对象;服务为 ftp 服务对象;时间表为 always 地址对象,代表任何时间;动作为 PERMIT 允许,如图 6-80 所示。




图 6-80　创建安全策略

创建完安全策略后,需要选择"启用"选项来使该规则生效,如图 6-81 所示。




图 6-81　启用安全策略

#### 4. 验证测试

在内部 PC 上安装好 FTP Server 程序,并进行相应的配置。在外部 PC 上测试到达

FTP 服务器的连通性,注意这里使用的 FTP 目标地址为 1.1.1.10。USG 将其发送到 1.1.1.10,端口为 21 的请求重定向到内部的 FTP 服务器,如图 6-82 所示。

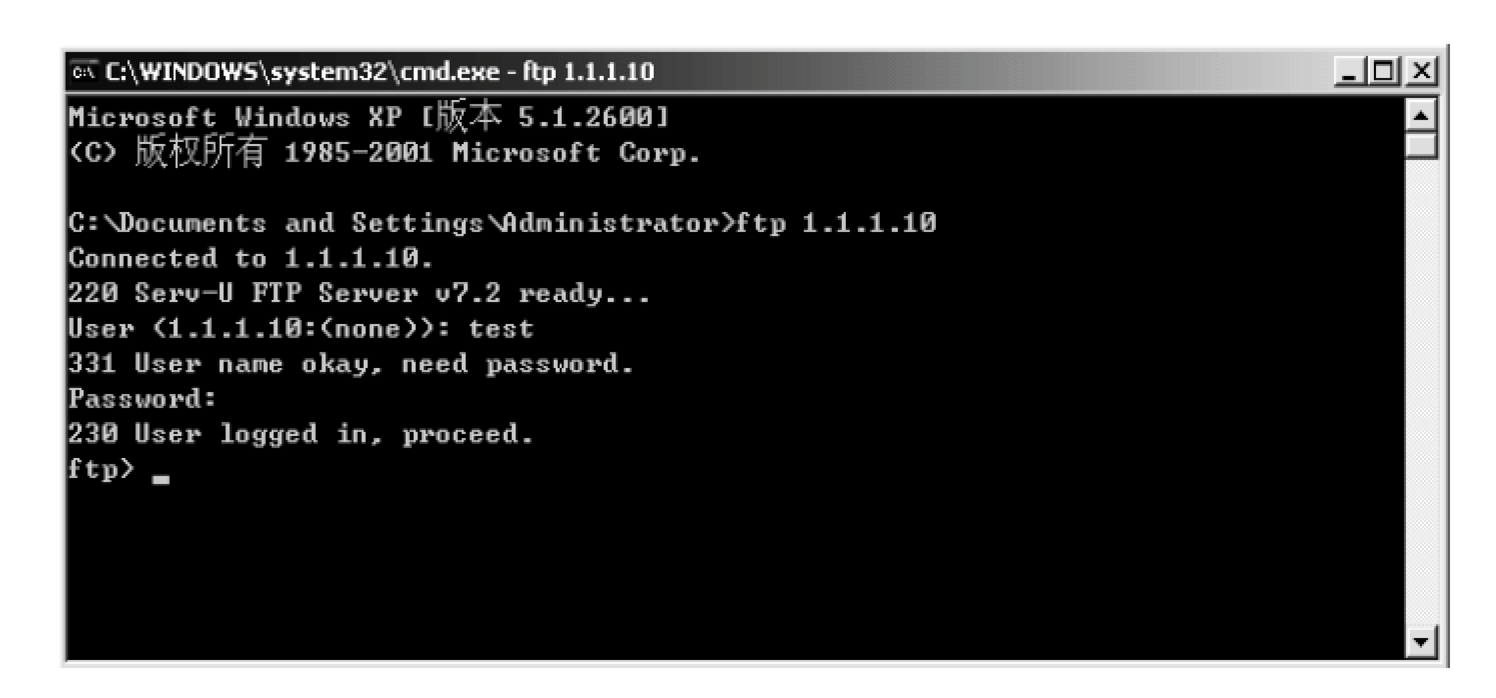



图 6-82　验证测试

外部 PC 可以通过预先设置的用户名和密码登录 FTP 服务器。

### 5. 实施 SYN Flood 攻击

在外部 PC 上使用 SYN Flood 连接工具以随机的源地址和端口向 FTP 服务器(1.1.1.10)发起攻击。此时在 FTP 服务器上通过 Windows 命令 netstat-an 可以看到外部主机与 FTP 服务器的 21 端口建立了大量的半开放连接,状态为 SYN_RECEIVED,如图 6-83 所示。

```
C:\WINDOWS\system32\cmd.exe
  TCP    192.168.1.10:21        1.251.96.101:9800      SYN_RECEIVED
  TCP    192.168.1.10:21        2.152.66.178:3359      SYN_RECEIVED
  TCP    192.168.1.10:21        2.191.216.79:38253     SYN_RECEIVED
  TCP    192.168.1.10:21        2.215.232.57:11348     SYN_RECEIVED
  TCP    192.168.1.10:21        3.76.115.230:1334      SYN_RECEIVED
  TCP    192.168.1.10:21        6.140.126.135:30804    SYN_RECEIVED
  TCP    192.168.1.10:21        7.84.241.58:62055      SYN_RECEIVED
  TCP    192.168.1.10:21        8.97.64.20:45395       SYN_RECEIVED
  TCP    192.168.1.10:21        8.220.243.168:36183    SYN_RECEIVED
  TCP    192.168.1.10:21        18.208.70.255:63255    SYN_RECEIVED
  TCP    192.168.1.10:21        19.11.230.252:62739    SYN_RECEIVED
  TCP    192.168.1.10:21        19.164.117.224:46196   SYN_RECEIVED
  TCP    192.168.1.10:21        20.153.205.211:3455    SYN_RECEIVED
  TCP    192.168.1.10:21        21.29.154.149:49408    SYN_RECEIVED
  TCP    192.168.1.10:21        21.66.0.38:65049       SYN_RECEIVED
  TCP    192.168.1.10:21        21.248.70.106:1072     SYN_RECEIVED
  TCP    192.168.1.10:21        22.114.114.230:7488    SYN_RECEIVED
  TCP    192.168.1.10:21        27.40.97.201:50520     SYN_RECEIVED
  TCP    192.168.1.10:21        28.219.174.50:8193     SYN_RECEIVED
  TCP    192.168.1.10:21        31.3.90.125:2373       SYN_RECEIVED
  TCP    192.168.1.10:21        33.219.125.90:59980    SYN_RECEIVED
  TCP    192.168.1.10:21        34.201.64.74:52554     SYN_RECEIVED
  TCP    192.168.1.10:21        34.244.204.207:54017   SYN_RECEIVED
  TCP    192.168.1.10:21        34.246.34.145:40256    SYN_RECEIVED
  TCP    192.168.1.10:21        35.91.87.237:15928     SYN_RECEIVED
```

图 6-83　实施 SYN Flood 攻击

### 6. 配置安全防护表

进入 USG 配置页面,即"安全策略"页面。选择"安全防护表"选项卡,如图 6-84 所示。

单击"新建"按钮创建安全防护表。为安全防护表配置名称,选择并展开"防 Flood 攻击"选项,选择 TCP Flood 中的"对目标主机限制最大连接"选项,并设置连接数为 15,如图 6-85 所示。

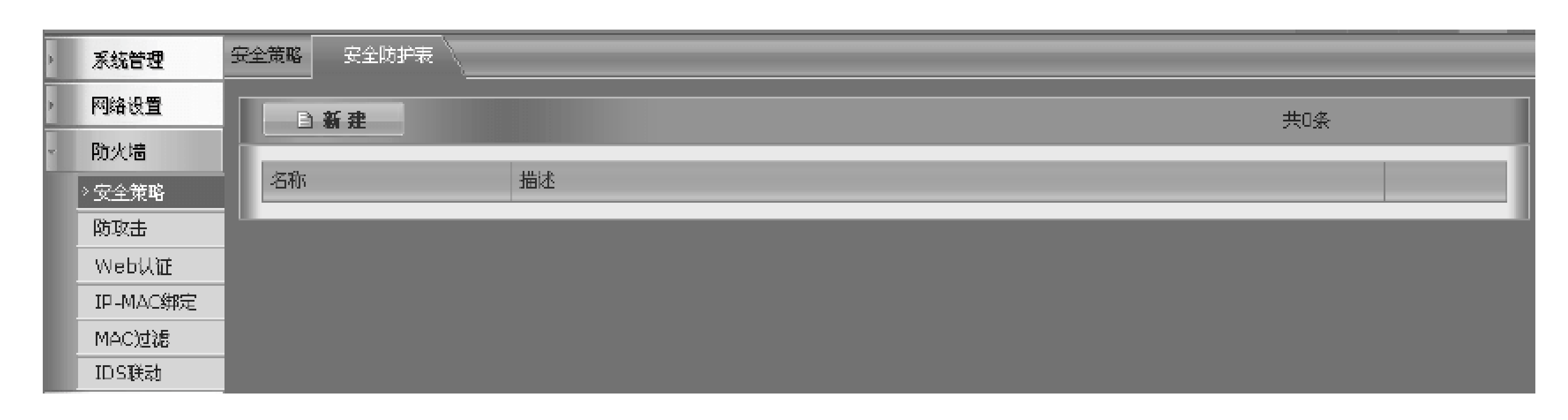



图 6-84　配置安全防护表

新建安全防护表

名称　DoS

描述

入侵防御

防病毒

Web过滤

邮件过滤

防Flood攻击

| | | 限制数量 |
|---|---|---|
| TCP Flood | | 限制数量 |
| | 对每台源主机进行流限制 | 100 |
| | ☑ 对目标主机限制最大连接 | 15 |
| UDP Flood | | 限制数量 |
| | 对每台源主机进行流限制 | 100 |
| | 对目标主机限制最大连接 | 40 |
| ICMP Flood | | 限制数量 |
| | 对每台源主机进行流限制 | 100 |
| | 对目标主机限制最大连接 | 40 |

图 6-85　创建安全防护表

配置完防 Flood 攻击后，仍然在该防护表中选择并展开“日志”选项，选择本地日志中的“防 Flood 攻击”选项，记录本地日志，如图 6-86 和图 6-87 所示。

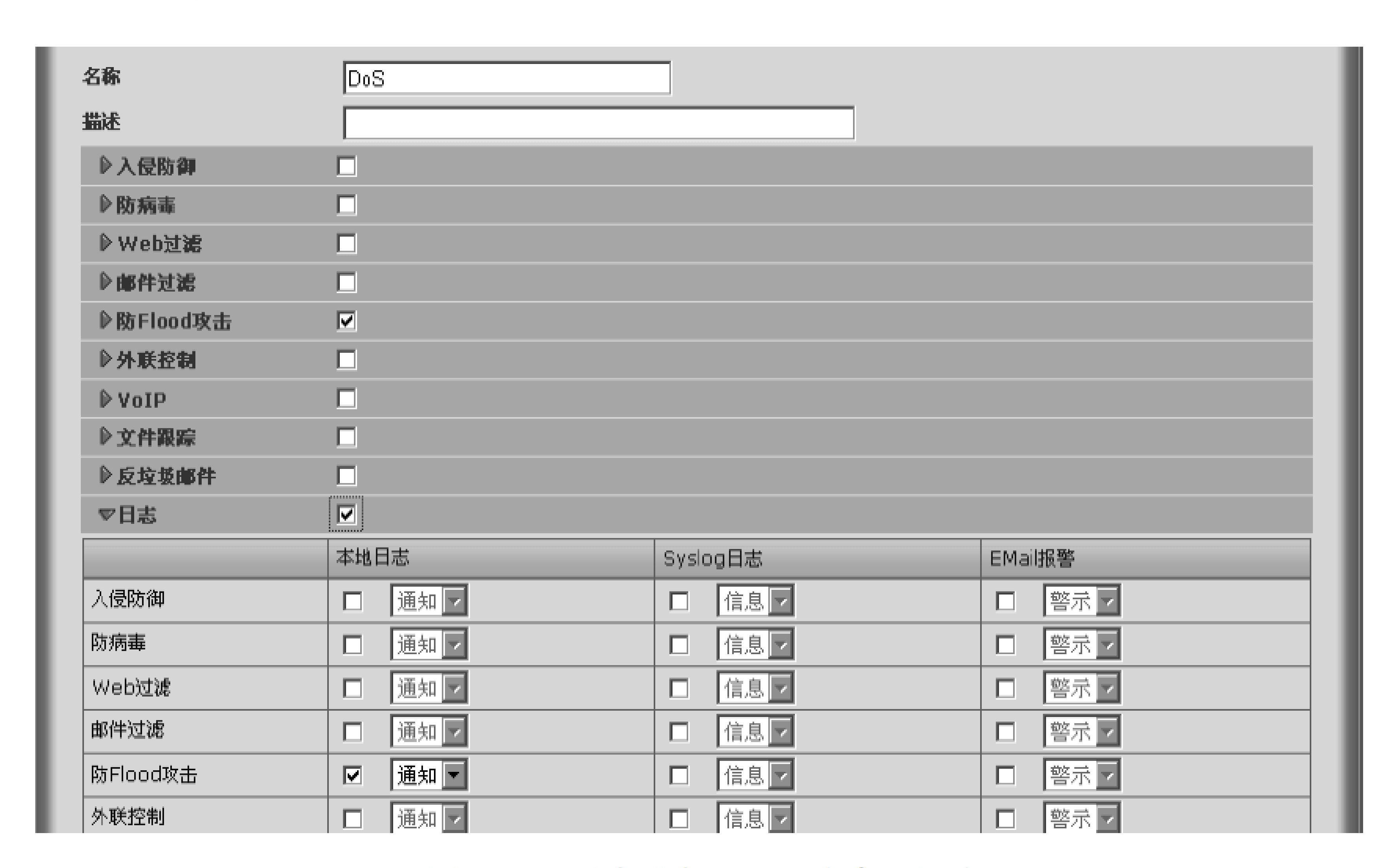



图 6-86　选择“防 Flood 攻击”选项

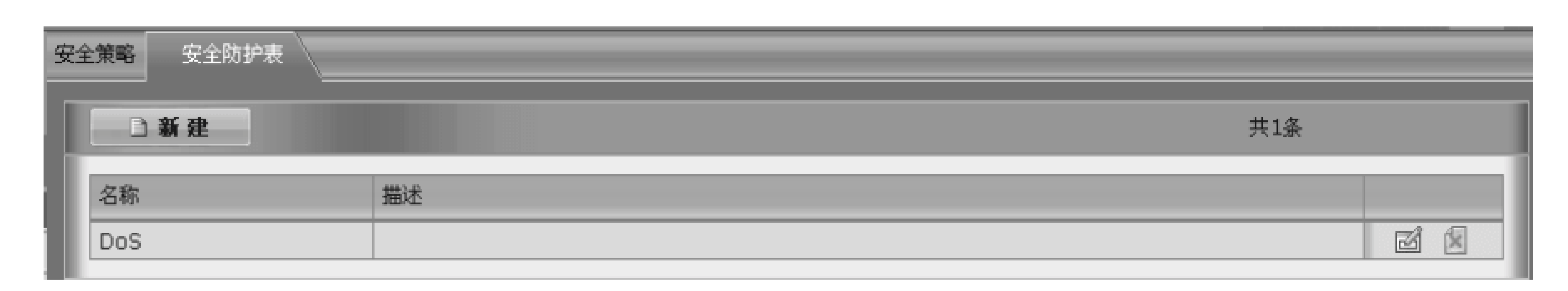



图 6-87　记录本地日志

### 7. 将安全防护表应用到安全策略

进入 USG 配置页面，即“安全策略”页面，对之前创建的安全策略进行编辑，在“安全防护”页面上引用刚创建的安全防护表，如图 6-88 和图 6-89 所示。




图 6-88　编辑安全策略(1)




图 6-89　编辑安全策略(2)

### 8. 配置本地日志

进入 USG 配置页面，即“日志配置”页面，选择“日志过滤”选项卡，在攻击事件中选择“DoS 事件”，以显示 DoS 攻击产生的日志，如图 6-90 所示。

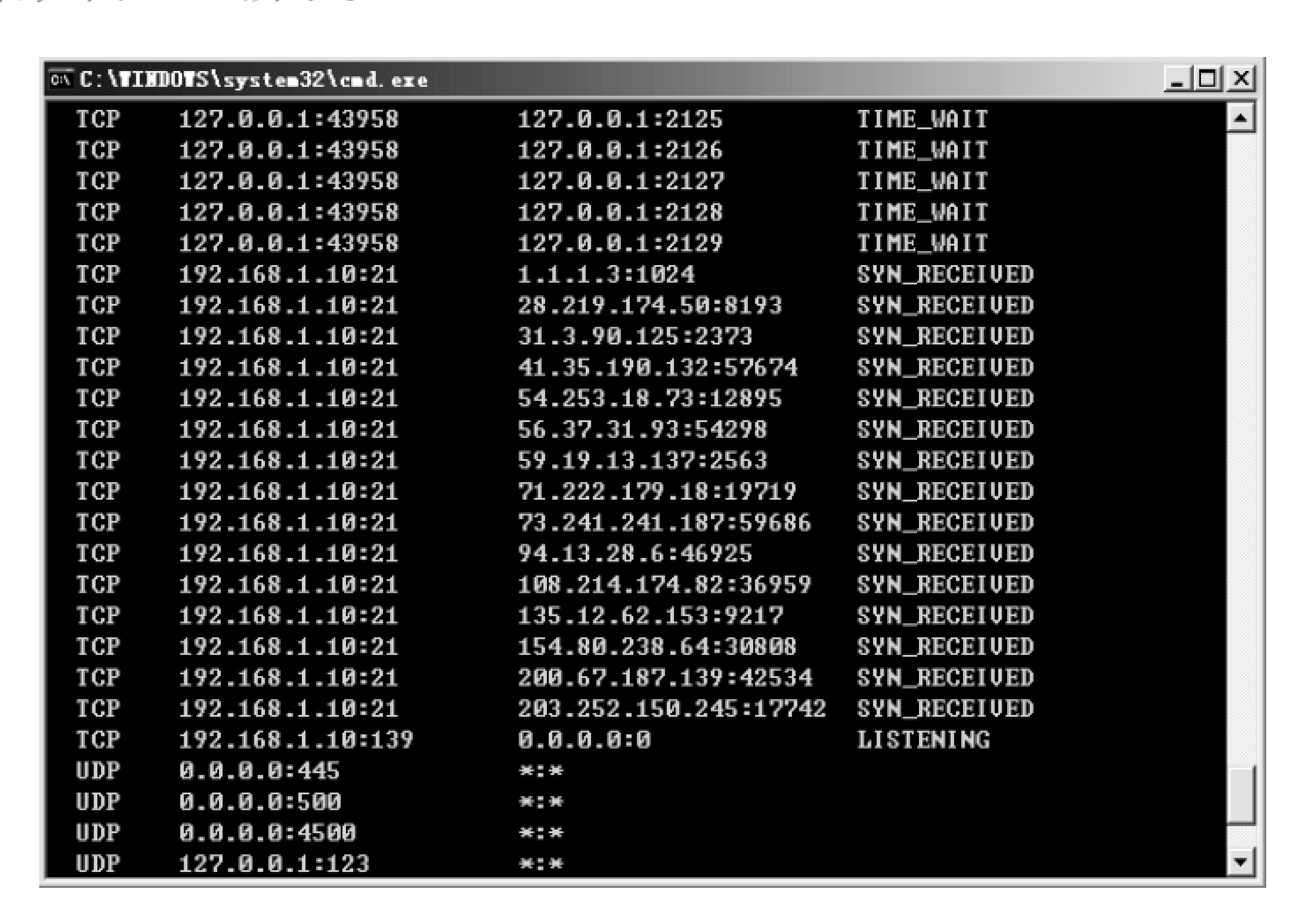
### 9. 验证测试

在外部 PC 上使用 SYN Flood 连接工具再次向 FTP 服务器(1.1.1.10)发起攻击。

| | 本地日志 | | Syslog日志 | | E-mail报警 | |
|---|---|---|---|---|---|---|
| 统一设置 | ☐ | | ☐ | | ☐ | |
| ▽ 防火墙事件 | | | | | | |
| NAT | ☐ | 通知 | ☐ | 紧急 | ☐ | 紧急 |
| DHCP(服务器/中继) | ☐ | 通知 | ☐ | 紧急 | ☐ | 紧急 |
| HA事件 | ☐ | 通知 | ☐ | 紧急 | ☐ | 紧急 |
| Web认证 | ☐ | 通知 | ☐ | 紧急 | ☐ | 紧急 |
| 运行信息 | ☐ | 通知 | ☐ | 紧急 | ☐ | 紧急 |
| 接口信息 | ☐ | 通知 | ☐ | 紧急 | ☐ | 紧急 |
| 系统事件 | ☐ | 通知 | ☐ | 紧急 | ☐ | 紧急 |
| 会话管理 | ☐ | 通知 | ☐ | 紧急 | ☐ | 紧急 |
| OSPF事件 | ☐ | 通知 | ☐ | 紧急 | ☐ | 紧急 |
| RIP事件 | ☐ | 通知 | ☐ | 紧急 | ☐ | 紧急 |
| DDNS | ☐ | 通知 | ☐ | 紧急 | ☐ | 紧急 |
| 二层过滤 | ☐ | 通知 | ☐ | 紧急 | ☐ | 紧急 |
| 流量控制 | ☐ | 通知 | ☐ | 紧急 | ☐ | 紧急 |
| 流量统计 | ☐ | 通知 | ☐ | 紧急 | ☐ | 紧急 |
| IDS联动 | ☐ | 通知 | ☐ | 紧急 | ☐ | 紧急 |
| ▽ 攻击事件 | | | | | | |
| DoS事件 | ☑ | 通知 | ☐ | 紧急 | ☐ | 紧急 |
| 扫描事件 | ☐ | 通知 | ☐ | 紧急 | ☐ | 紧急 |

图 6-90　配置本地日志

此时在 FTP 服务器上通过 Windows 命令 netstat-an 可以看到外部主机与 FTP 服务器的 21 端口只建立了少量的半开放连接(大约 15 个),其他所有的 SYN Flood 攻击报文已经被 USG 阻断,如图 6-91 所示。



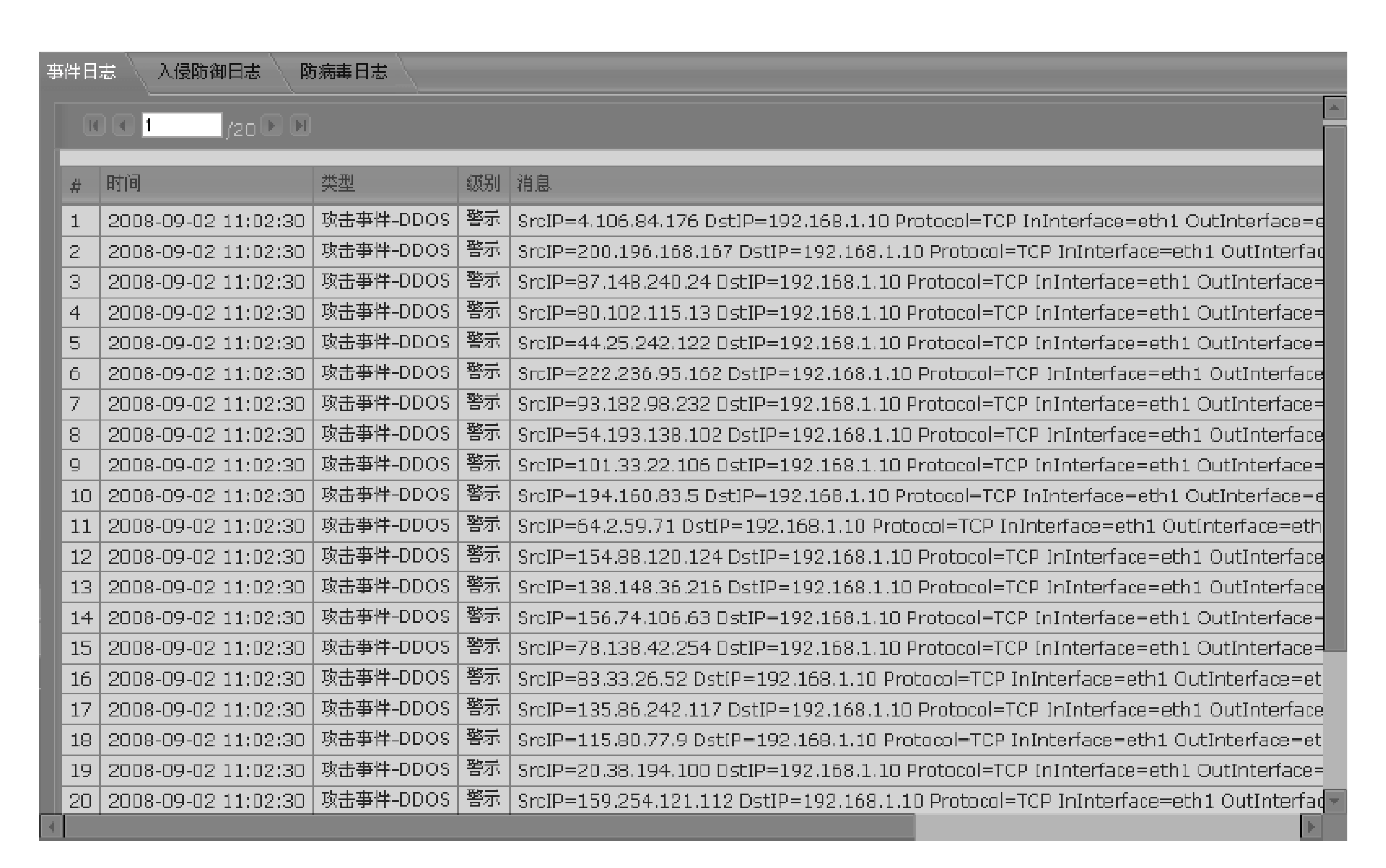
```
C:\WINDOWS\system32\cmd.exe
TCP    127.0.0.1:43958      127.0.0.1:2125        TIME_WAIT
TCP    127.0.0.1:43958      127.0.0.1:2126        TIME_WAIT
TCP    127.0.0.1:43958      127.0.0.1:2127        TIME_WAIT
TCP    127.0.0.1:43958      127.0.0.1:2128        TIME_WAIT
TCP    127.0.0.1:43958      127.0.0.1:2129        TIME_WAIT
TCP    192.168.1.10:21      1.1.1.3:1024          SYN_RECEIVED
TCP    192.168.1.10:21      28.219.174.50:8193    SYN_RECEIVED
TCP    192.168.1.10:21      31.3.90.125:2373      SYN_RECEIVED
TCP    192.168.1.10:21      41.35.190.132:57674   SYN_RECEIVED
TCP    192.168.1.10:21      54.253.18.73:12895    SYN_RECEIVED
TCP    192.168.1.10:21      56.37.31.93:54298     SYN_RECEIVED
TCP    192.168.1.10:21      59.19.13.137:2563     SYN_RECEIVED
TCP    192.168.1.10:21      71.222.179.18:19719   SYN_RECEIVED
TCP    192.168.1.10:21      73.241.241.187:59686  SYN_RECEIVED
TCP    192.168.1.10:21      94.13.28.6:46925      SYN_RECEIVED
TCP    192.168.1.10:21      108.214.174.82:36959  SYN_RECEIVED
TCP    192.168.1.10:21      135.12.62.153:9217    SYN_RECEIVED
TCP    192.168.1.10:21      154.80.238.64:30808   SYN_RECEIVED
TCP    192.168.1.10:21      200.67.187.139:42534  SYN_RECEIVED
TCP    192.168.1.10:21      203.252.150.245:17742 SYN_RECEIVED
TCP    192.168.1.10:139     0.0.0.0:0             LISTENING
UDP    0.0.0.0:445          *:*
UDP    0.0.0.0:500          *:*
UDP    0.0.0.0:4500         *:*
UDP    127.0.0.1:123        *:*
```

图 6-91　验证测试

进入 USG 配置页面,即“本地日志”页面,选择“事件日志”选项卡,可以看到之前 DoS 攻击产生的日志,如图 6-92 所示。

## 【注意事项】

本实验涉及的攻击工具只能用于实验。




| # | 时间 | 类型 | 级别 | 消息 |
|---|---|---|---|---|
| 1 | 2008-09-02 11:02:30 | 攻击事件-DDOS | 警示 | SrcIP=4.106.84.176 DstIP=192.168.1.10 Protocol=TCP InInterface=eth1 OutInterface=e |
| 2 | 2008-09-02 11:02:30 | 攻击事件-DDOS | 警示 | SrcIP=200.196.168.167 DstIP=192.168.1.10 Protocol=TCP InInterface=eth1 OutInterfac |
| 3 | 2008-09-02 11:02:30 | 攻击事件-DDOS | 警示 | SrcIP=87.148.240.24 DstIP=192.168.1.10 Protocol=TCP InInterface=eth1 OutInterface= |
| 4 | 2008-09-02 11:02:30 | 攻击事件-DDOS | 警示 | SrcIP=80.102.115.13 DstIP=192.168.1.10 Protocol=TCP InInterface=eth1 OutInterface= |
| 5 | 2008-09-02 11:02:30 | 攻击事件-DDOS | 警示 | SrcIP=44.25.242.122 DstIP=192.168.1.10 Protocol=TCP InInterface=eth1 OutInterface= |
| 6 | 2008-09-02 11:02:30 | 攻击事件-DDOS | 警示 | SrcIP=222.236.95.162 DstIP=192.168.1.10 Protocol=TCP InInterface=eth1 OutInterface |
| 7 | 2008-09-02 11:02:30 | 攻击事件-DDOS | 警示 | SrcIP=93.182.98.232 DstIP=192.168.1.10 Protocol=TCP InInterface=eth1 OutInterface= |
| 8 | 2008-09-02 11:02:30 | 攻击事件-DDOS | 警示 | SrcIP=54.193.138.102 DstIP=192.168.1.10 Protocol=TCP InInterface=eth1 OutInterface |
| 9 | 2008-09-02 11:02:30 | 攻击事件-DDOS | 警示 | SrcIP=101.33.22.106 DstIP=192.168.1.10 Protocol=TCP InInterface=eth1 OutInterface= |
| 10 | 2008-09-02 11:02:30 | 攻击事件-DDOS | 警示 | SrcIP=194.160.83.5 DstIP=192.168.1.10 Protocol=TCP InInterface=eth1 OutInterface=e |
| 11 | 2008-09-02 11:02:30 | 攻击事件-DDOS | 警示 | SrcIP=64.2.59.71 DstIP=192.168.1.10 Protocol=TCP InInterface=eth1 OutInterface=eth |
| 12 | 2008-09-02 11:02:30 | 攻击事件-DDOS | 警示 | SrcIP=154.88.120.124 DstIP=192.168.1.10 Protocol=TCP InInterface=eth1 OutInterface |
| 13 | 2008-09-02 11:02:30 | 攻击事件-DDOS | 警示 | SrcIP=138.148.36.216 DstIP=192.168.1.10 Protocol=TCP InInterface=eth1 OutInterface |
| 14 | 2008-09-02 11:02:30 | 攻击事件-DDOS | 警示 | SrcIP=156.74.106.63 DstIP=192.168.1.10 Protocol=TCP InInterface=eth1 OutInterface= |
| 15 | 2008-09-02 11:02:30 | 攻击事件-DDOS | 警示 | SrcIP=78.138.42.254 DstIP=192.168.1.10 Protocol=TCP InInterface=eth1 OutInterface= |
| 16 | 2008-09-02 11:02:30 | 攻击事件-DDOS | 警示 | SrcIP=83.33.26.52 DstIP=192.168.1.10 Protocol=TCP InInterface=eth1 OutInterface=et |
| 17 | 2008-09-02 11:02:30 | 攻击事件-DDOS | 警示 | SrcIP=135.86.242.117 DstIP=192.168.1.10 Protocol=TCP InInterface=eth1 OutInterface |
| 18 | 2008-09-02 11:02:30 | 攻击事件-DDOS | 警示 | SrcIP=115.80.77.9 DstIP=192.168.1.10 Protocol=TCP InInterface=eth1 OutInterface=et |
| 19 | 2008-09-02 11:02:30 | 攻击事件-DDOS | 警示 | SrcIP=20.38.194.100 DstIP=192.168.1.10 Protocol=TCP InInterface=eth1 OutInterface= |
| 20 | 2008-09-02 11:02:30 | 攻击事件-DDOS | 警示 | SrcIP=159.254.121.112 DstIP=192.168.1.10 Protocol=TCP InInterface=eth1 OutInterfac |

图 6-92　DoS 攻击产生日志

## 6.5　使用统一安全网关限制 IM 软件

### 【实验名称】

使用统一安全网关限制 IM 软件。

### 【实验目的】

使用(USG)统一安全网关限制即时通信软件(IM)，对 IM 软件进行管理。

### 【背景描述】

某企业为了提高网络的安全性，部署了一台 USG。但是，公司发现许多员工在工作时间，使用即时通信软件(例如 QQ)进行聊天，严重影响了工作效率。公司希望在上班时间不允许普通员工使用 IM 软件进行聊天，只有广告部的员工由于业务需要可以使用 IM 软件。

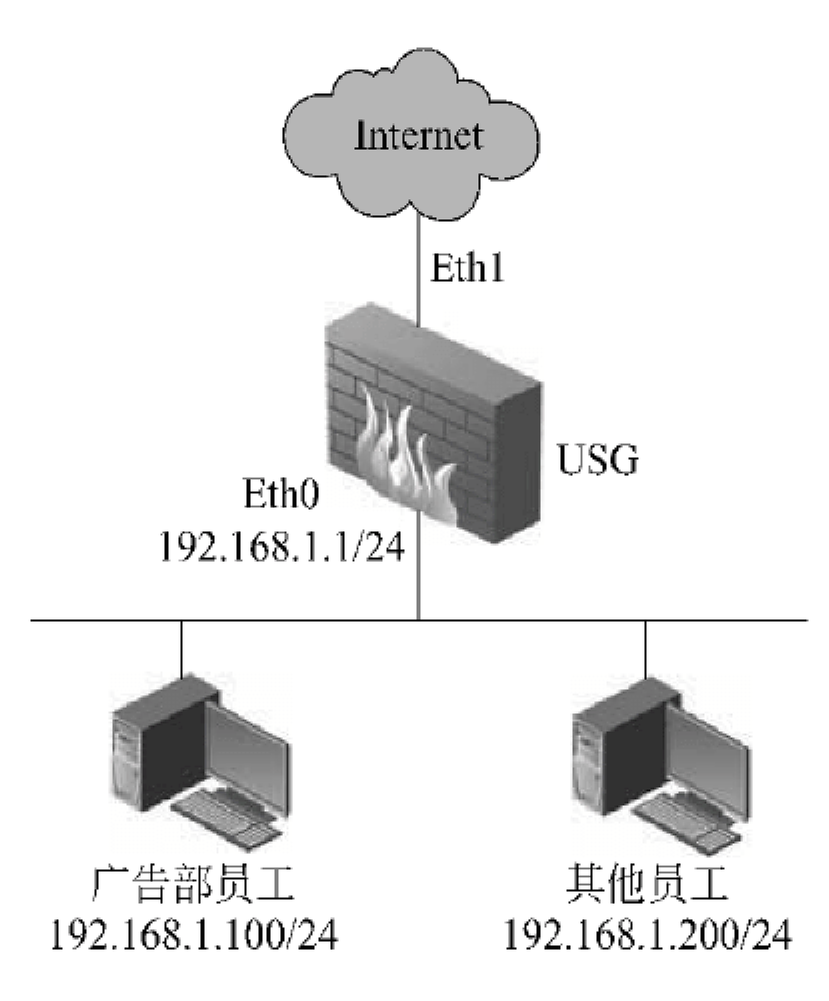



图 6-93　统一安全网关限制 IM 软件网络拓扑图

### 【需求分析】

为了实现对 IM 软件的限制，可以使用 USG 的 IM 软件管理功能，只允许特定的 IM 用户登录。

### 【实验拓扑】

如图 6-93 所示的网络拓扑，是企业网络管理

员发现许多员工在工作时间，使用即时通信软件(例如 QQ)进行聊天，严重影响了工作效率。公司希望在上班时间不允许普通员工使用 IM 软件进行聊天，只有广告部的员工由于业务需要，可以使用 IM 软件。为了提高网络的效率，购买了一台 RG-USG 统一安全网关，使用 USG 的 IM 软件管理功能，只允许特定的 IM 用户登录。

## 【实验设备】

USG 连接到 Internet 的链路
USG　1 台
PC　　2 台

## 【预备知识】

- 网络基础知识。
- USG 操作基础知识。

## 【实验原理】

USG 支持对 IM 软件进行管理的功能。USG 可以对 MSN、QQ、雅虎通等 IM 软件进行限制，只允许特定的用户使用 IM 软件。

本实验以 QQ 软件为例。

## 【实验步骤】

### 1. 配置 USG接口的 IP地址

如图 6-94 所示，进入 USG 的配置页面，即“接口”页面。

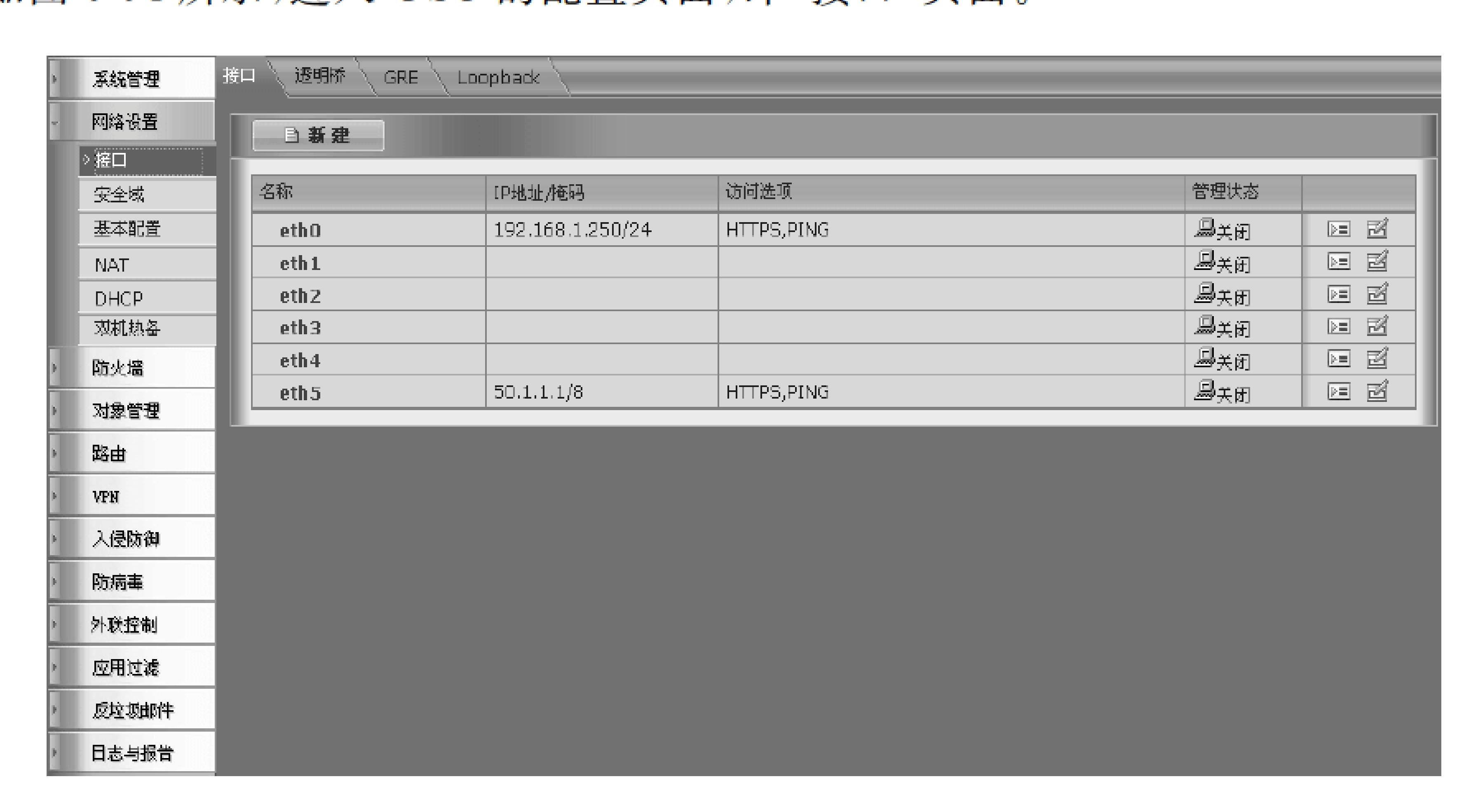



图 6-94　进入 USG 的配置页面

单击 eth0 接口的“编辑”图标，为 eth0 接口配置 IP 地址及子网掩码，如图 6-95 所示。

单击 eth1 接口的“编辑”图标，为 eth1 接口配置 IP 地址及子网掩码。这里 eth1 接口作为连接到 Internet 的接口，请根据实际情况配置 eth1 接口的地址信息。




图 6-95　eth0 接口配置 IP 地址

## 2. 配置 USG 的默认网关

进入 USG 的配置页面，即“基本配置”页面，在网关地址栏中，请根据实际情况配置访问 Internet 的默认网关地址，如图 6-96 所示。




图 6-96　配置 USG 的默认网关

## 3. 配置内部子网的地址对象

进入 USG 的配置页面，即“地址对象”页面，可以看到系统预定义了一个名为 any 的地址对象，它包括所有的地址 0.0.0.0/0，如图 6-97 所示。

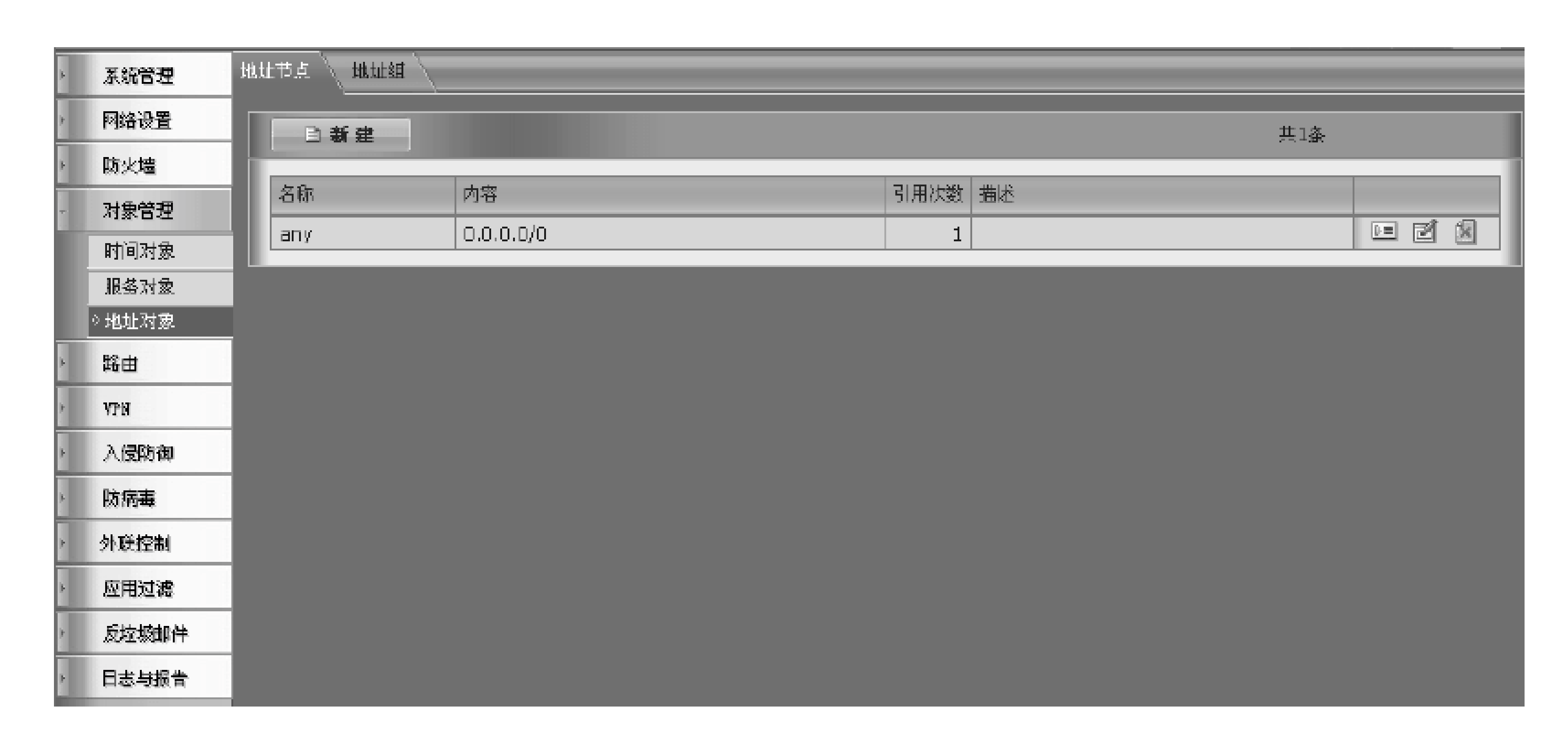



图 6-97　配置内部子网的地址对象

单击“新建”按钮创建地址对象，该地址对象包括公司内部子网 192.168.1.0/24，如图 6-98 所示。




图 6-98　创建地址对象

## 4. 配置 NAT

进入 USG 的配置页面，即 NAT 页面，单击“新建”按钮创建 NAT 规则。

NAT 规则中的源地址选择之前创建的 inside 地址对象，目标地址使用 any 地址对象，服务使用 any 服务对象，出接口为连接 Internet 的 eth1 接口，转换后源地址为“出接口地址”，即 eth1 接口的地址，如图 6-99 和图 6-100 所示。




图 6-99　创建 NAT 规则(1)




图 6-100　创建 NAT 规则(2)

## 5. 配置安全防护表

进入 USG 配置页面，即“安全策略”页面，选择“安全防护表”选项卡，如图 6-101

所示。




图 6-101　配置安全防护表

单击“新建”按钮创建安全防护表。为安全防护表配置名称，选择并展开“外联控制”选项，勾选 IM 复选框，如图 6-102 和图 6-103 所示。




图 6-102　创建安全防护表




图 6-103　选择展开外联控制

## 6. 配置安全策略

进入 USG 配置页面，即“安全策略”页面，如图 6-104 所示。

单击“新建”按钮创建安全策略。在安全策略中源接口为 eth0 接口；源地址为 inside 地址对象；目的接口为 eth1 接口；目的地址为 any 地址对象；服务为 any 服务对象；时间表为 always 地址对象，代表任何时间；动作为 PERMIT 允许；“安全防护”选择之前创建的安全防护表 QQ ，如图 6-105 所示。

创建完安全策略后，需要选择“启用”选项来使该规则生效，如图 6-106 所示。




图 6-104　配置安全策略




图 6-105　创建的 QQ 安全防护表




图 6-106　启用安全策略

## 7. 验证测试

在广告部的 PC 上和其他员工的 PC 上登录 QQ 软件，都可以登录成功。

进入 USG 配置页面，即 IM 页面，选择“监视器”选项卡，可以查看登录 IM 用户的详细信息。例如协议、用户名、IP 地址等，如图 6-107 所示。




图 6-107　验证测试

从图 6-107 中可以看到，广告部 PC 和其他员工的 PC 都成功登录了 QQ。

## 8. 配置 IM白名单

现在需要进行 IM 限制的相关配置，只允许广告部员工登录 QQ。

进入 USG 配置页面，即 IM 页面，选择“白名单”选项卡，如图 6-108 所示。




图 6-108　配置 IM 白名单

单击“新建”按钮创建黑名单。在“协议”下拉列表中选择“QQ”；在“用户名”文本框中输入广告部员工的 QQ 号，并勾选“启用”复选框，如图 6-109 和图 6-110 所示。




图 6-109　创建黑名单

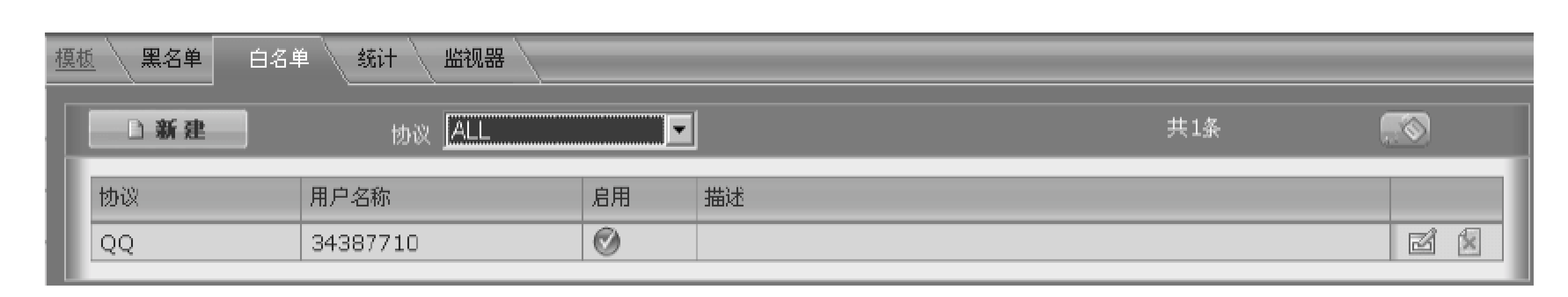



图 6-110　启用创建的黑名单

## 9. 配置 IM模板

进入 USG 配置页面，即 IM 页面，选择“模板”选项卡，如图 6-111 所示。




图 6-111　配置 IM 模板

单击“新建”按钮创建 IM 模板。为模板配置名称后，选择 QQ 选项，并选择“白名单”，如图 6-112 和图 6-113 所示。




图 6-112　创建 IM 模板

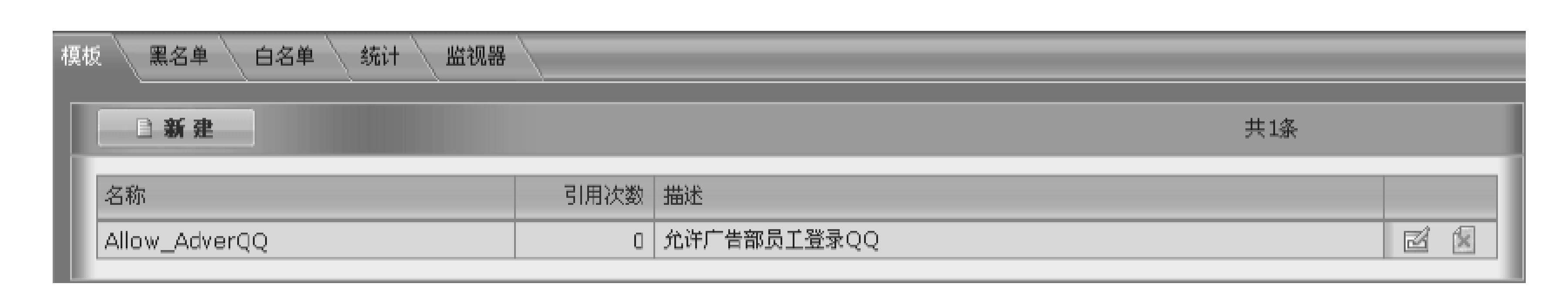



图 6-113　选择白名单

## 10. 配置安全防护表

进入 USG 配置页面，即“安全策略”页面，选择“安全防护表”选项卡，对之前创建的名为 QQ 的安全防护表进行编辑，使该防护表在外联控制的 IM 中引用之前创建的 IM 模板 Allow_AdverQQ，如图 6-114 所示。




图 6-114　配置安全防护表

## 11. 验证测试

在广告部的 PC 上和其他员工的 PC 上登录 QQ 软件，这时只有广告部的员工可以登录 QQ，其他员工则无法登录 QQ。

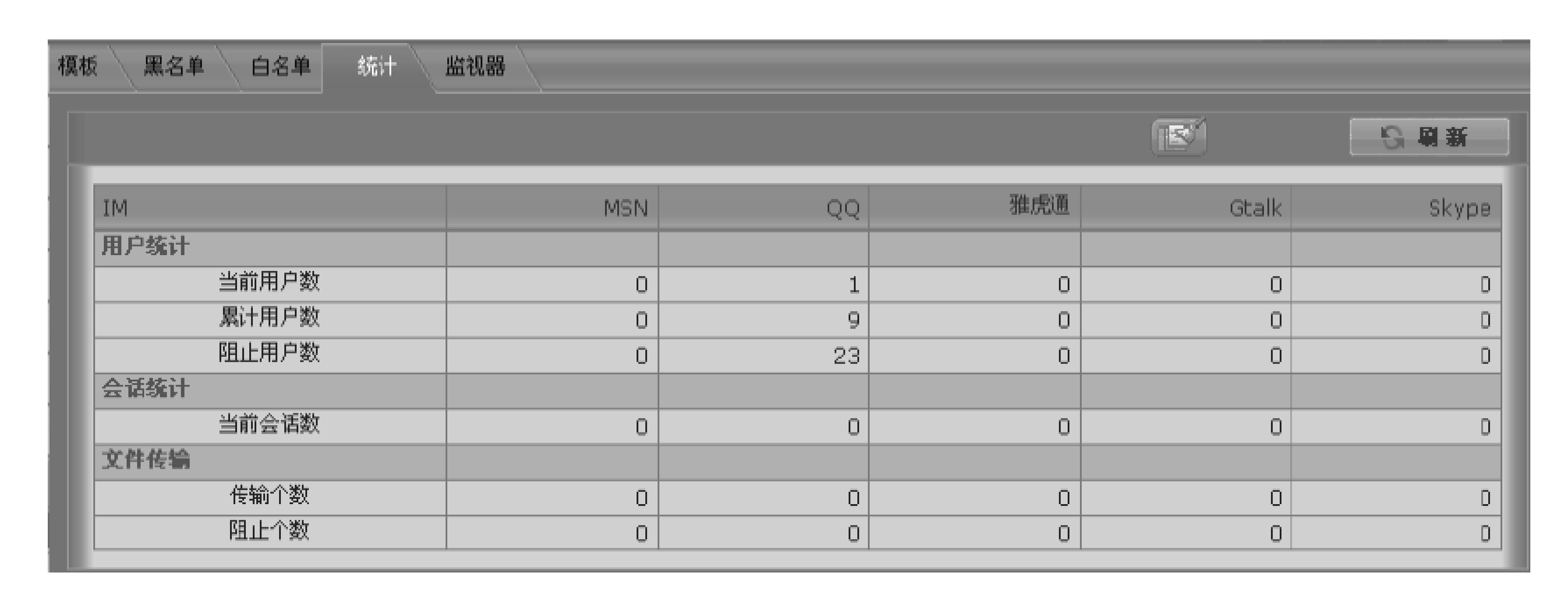
进入 USG 配置页面，即 IM 页面，选择“监视器”选项卡，可以看到广告部员工 QQ 登录的信息，如图 6-115 所示。




| # | 协议 | 用户名 | 所属名单 | 源IP | 最后登录时间 |
|---|---|---|---|---|---|
| 1 | QQ | 42309471 | 白名单 | 192.168.1.100 | 2008-09-01 14:29:56 |

图 6-115　验证测试

选择“统计”选项卡，可以查看被 USG 阻止的用户数等信息，如图 6-116 所示。




| IM | MSN | QQ | 雅虎通 | Gtalk | Skype |
|---|---|---|---|---|---|
| 用户统计 | | | | | |
| 当前用户数 | 0 | 1 | 0 | 0 | 0 |
| 累计用户数 | 0 | 9 | 0 | 0 | 0 |
| 阻止用户数 | 0 | 23 | 0 | 0 | 0 |
| 会话统计 | | | | | |
| 当前会话数 | 0 | 0 | 0 | 0 | 0 |
| 文件传输 | | | | | |
| 传输个数 | 0 | 0 | 0 | 0 | 0 |
| 阻止个数 | 0 | 0 | 0 | 0 | 0 |

图 6-116　查看被 USG 阻止的用户数信息

## 【注意事项】

- 在实验中，请根据实际情况配置 USG 到达 Internet 的连接。

• 本实验使用的是白名单，如果想阻断特定用户使用 IM 软件，可以使用黑名单进行配置。

## 6.6 使用统一安全网关过滤 Web 病毒

### 【实验名称】

使用统一安全网关过滤 Web 病毒。

### 【实验目的】

使用(USG)统一安全网关过滤 Web/HTTP 流量中的病毒。

### 【背景描述】

某企业为了提高网络的安全性，在网络出口处部署了一台 USG。但最近管理员发现，内部网络中的很多主机都被感染了病毒，而且经过分析和定位后，发现很多病毒都是嵌入在 HTTP 流量中，即用户浏览网页时会将病毒下载到本地。公司希望能够防止嵌入在 HTTP 流量中的病毒进入到内部网络中。

### 【需求分析】

为了防止网页病毒进入到内部网络中，需要在网关处进行病毒检测，阻止恶意的流量传输到内部网络中。

### 【实验拓扑】

如图 6-117 所示的网络拓扑，是企业为了提高网络的安全，在网络出口处部署了一台 USG。但最近管理员发现，内部网络中的很多主机都被感染了病毒，而且经过分析和定位后，发现很多病毒都是嵌入在 HTTP 流量中，公司希望能够防止嵌入在 HTTP 流量中的病毒进入到内部网络中，因此，购买了一台 RG-USG 统一安全网关，在网关处进行病毒检测，阻止恶意的流量传输到内部网络中，以实现网络的安全防范功能。

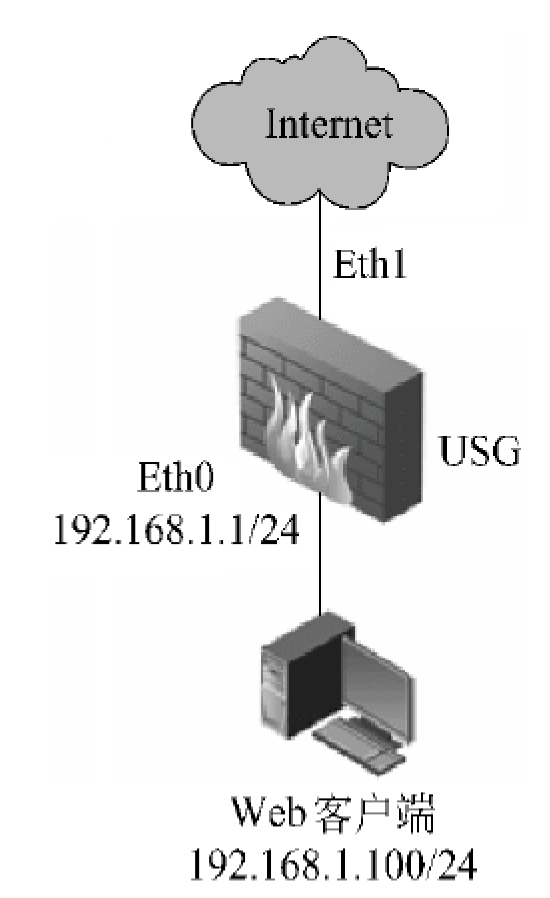



图 6-117 统一安全网关过滤 Web 病毒网络拓扑图

### 【实验设备】

USG 连接到 Internet 的链路
USG 1 台
PC 1 台

### 【预备知识】

• 网络基础知识。

• USG 操作基础知识。

## 【实验原理】

USG 集成了网关病毒过滤功能，支持对 Web/HTTP 流量进行病毒扫描，可以将 Web/HTTP 流量中的病毒过滤掉，保护内部网络免受病毒入侵。

## 【实验步骤】

### 1. 配置 USG 接口的 IP 地址

如图 6-118 所示，进入 USG 的配置页面，即“接口”页面。

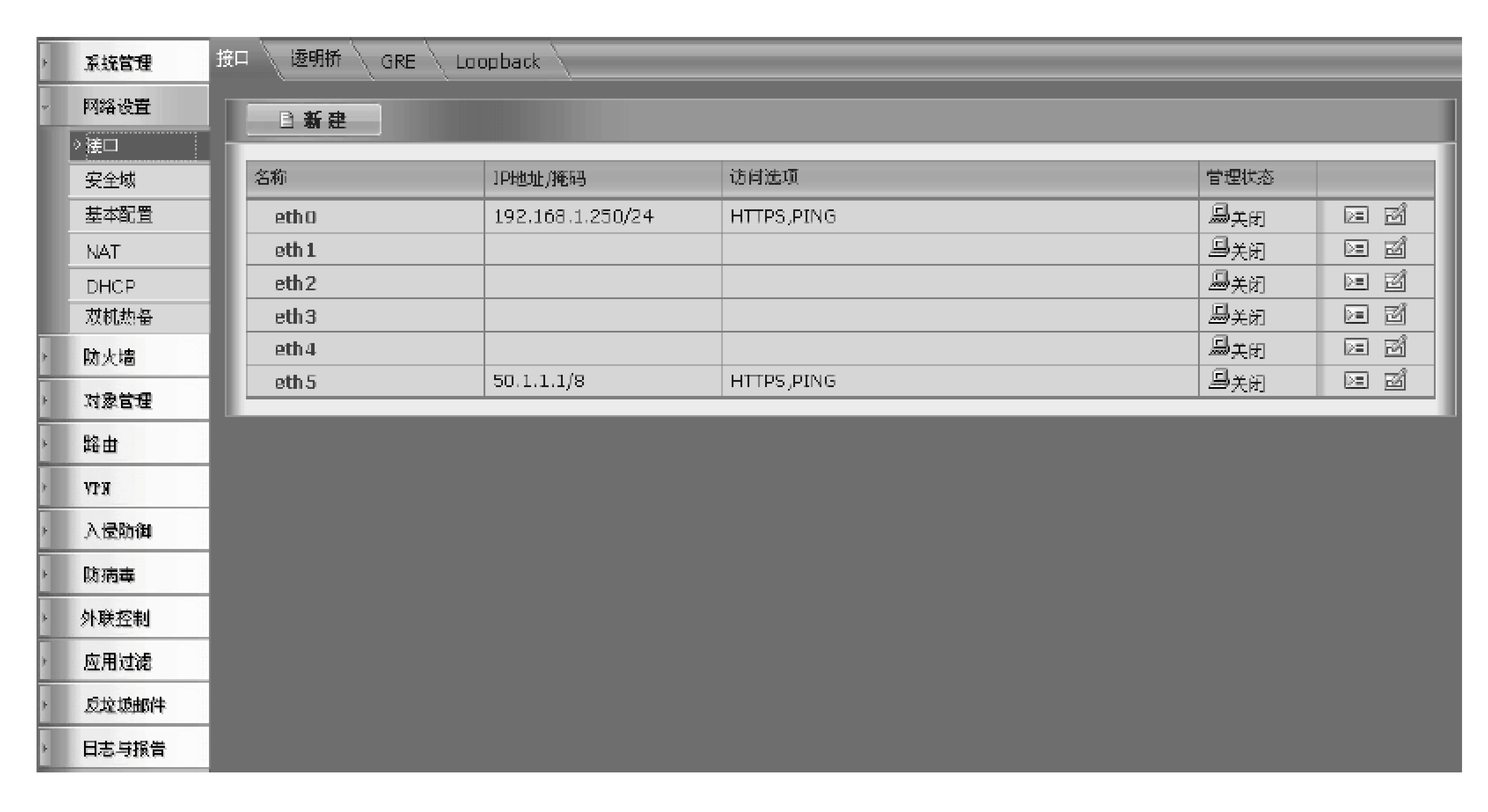



图 6-118　配置 USG 接口的 IP 地址

单击 eth0 接口的“编辑”图标，为 eth0 接口配置 IP 地址及子网掩码，如图 6-119 所示。




图 6-119　为 eth0 接口配置 IP 地址

单击 eth1 接口的“编辑”图标，为 eth1 接口配置 IP 地址及子网掩码。这里 eth1 接口作为连接到 Internet 的接口，请根据实际情况配置 eth1 接口的地址信息。

### 2. 配置 USG 的默认网关

进入 USG 的配置页面,即"基本配置"页面,在网关地址栏中,请根据实际情况配置访问 Internet 的默认网关地址,如图 6-120 所示。




图 6-120　配置 USG 的默认网关

### 3. 配置内部子网的地址对象

进入 USG 的配置页面,即"地址对象"页面,可以看到系统预定义了一个名为 any 的地址对象,它包括所有的地址 0.0.0.0/0,如图 6-121 所示。

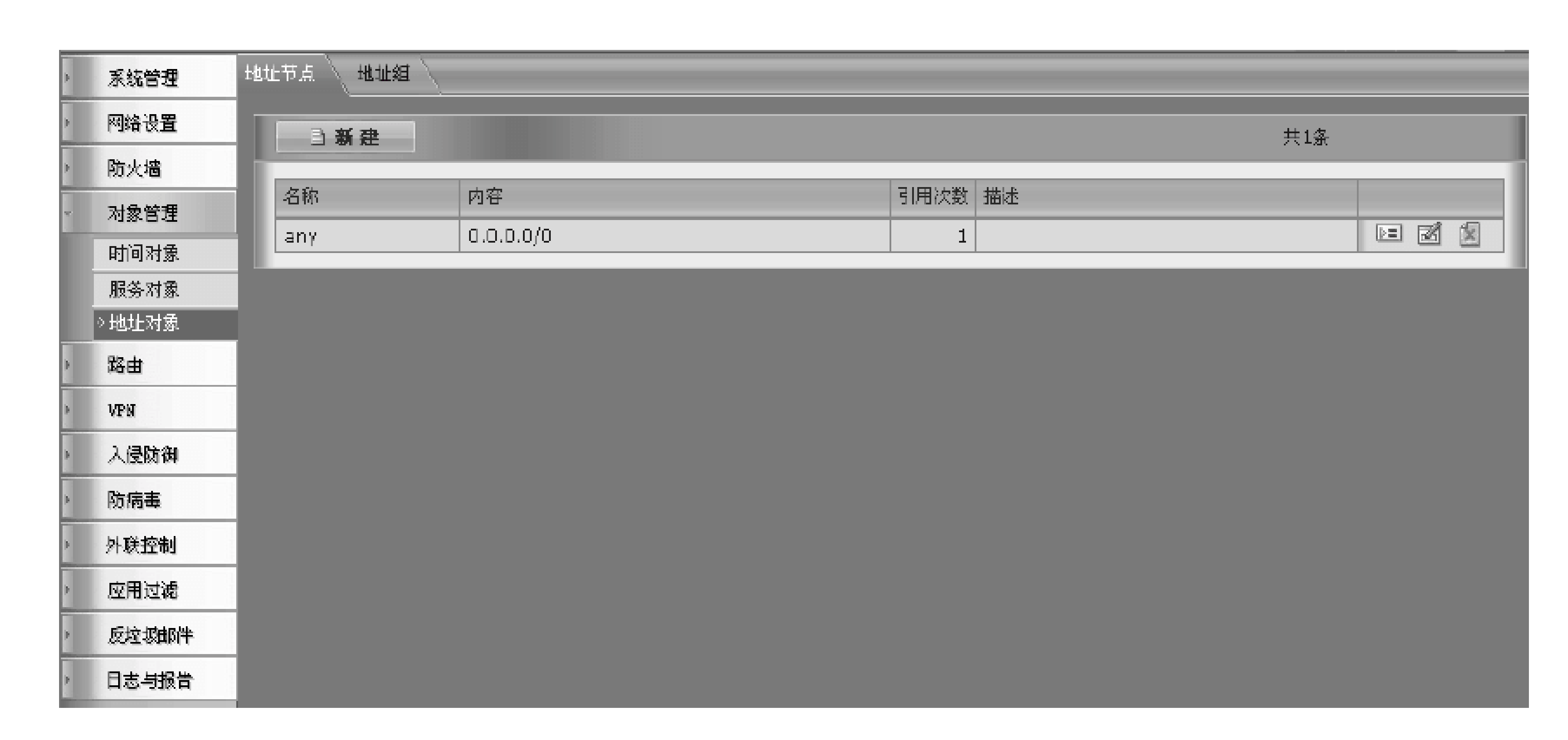



图 6-121　配置内部子网的地址对象

单击"新建"按钮创建地址对象,该地址对象包括公司内部子网 192.168.1.0/24,如图 6-122 所示。

### 4. 配置 NAT

进入 USG 的配置页面,即 NAT 页面,单击"新建"按钮创建 NAT 规则。

NAT 规则中的源地址选择之前创建的 inside 地址对象,目标地址使用 any 地址对象,服务使用 any 服务对象,出接口为连接 Internet 的 eth1 接口,转换后源地址为"出接口地址",即 eth1 接口的地址,如图 6-123 和图 6-124 所示。

### 5. 配置安全策略

进入 USG 配置页面,即"安全策略"页面,如图 6-125 所示。




图 6-122　创建地址对象




图 6-123　配置 NAT 规则(1)




图 6-124　配置 NAT 规则(2)




图 6-125　配置安全策略

单击“新建”按钮创建安全策略。在安全策略中源接口为eth0接口;源地址为inside地址对象;目的接口为eth1接口;目的地址为any地址对象;服务为any服务对象;时间表为always地址对象,代表任何时间;动作为PERMIT允许,如图6-126所示。




图6-126 创建安全策略

创建完安全策略后,需要选择“启用”选项来使该规则生效,如图6-127所示。




图6-127 启用安全策略

## 6. 验证测试

在内部PC上访问带有病毒的网页(该病毒文件名为eicar.com),并将病毒使用HTTP进行下载,如图6-128所示。

**注意**:这时如果PC上安装了可以检测出该病毒的杀毒软件,则杀毒软件会进行告警,并阻止下载病毒,如图6-129所示。

## 7. 配置防病毒

进入USG配置页面,即“文件扫描列表”页面,选择需要进行病毒扫描的文件类型,如图6-130所示。

## 8. 配置安全防护表

进入USG配置页面,即“安全策略”页面,选择“安全防护表”选项卡,如图6-131所示。




图 6-128　下载病毒




图 6-129　检测出该病毒

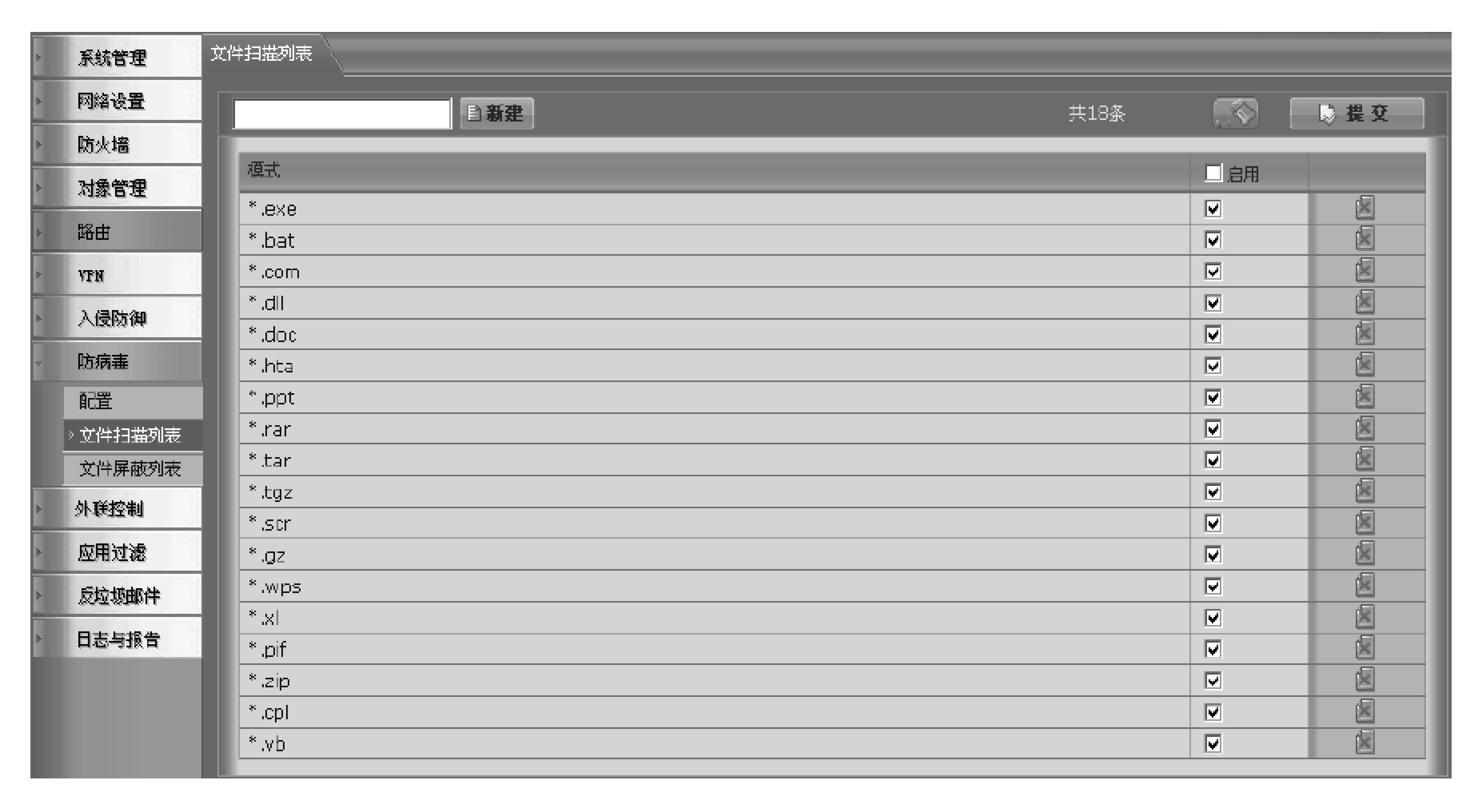



图 6-130　选择需要进行病毒扫描的文件类型




图 6-131　配置安全防护表

单击“新建”按钮创建安全防护表。为安全防护表配置名称，选择并展开“防病毒”选项，选择对 HTTP 流量进行文件扫描，如图 6-132 所示。

图 6-132　创建安全防护表

仍然在该防护表中选择并展开“日志”选项，选择本地日志中的“防病毒”选项，记录本地日志，如图 6-133 和图 6-134 所示。




图 6-133　选择本地日志中的“防病毒”选项




图 6-134　记录本地日志

### 9. 将安全防护表应用到安全策略

进入 USG 配置页面,即“安全策略”页面,对之前创建的安全策略进行编辑,在“安全防护”下拉列表中选择刚创建的安全防护表,如图 6-135 和图 6-136 所示。




图 6-135　创建的安全策略(1)




图 6-136　创建的安全策略(2)

### 10. 验证测试

在内部 PC 上再次访问之前带有病毒的网页(该病毒文件名为 eicar.com),并将病毒使用 HTTP 进行下载。这时可以看到无法下载,因为 USG 已经将病毒过滤,如图 6-137 所示。

同时进入 USG 配置页面,即“本地日志”页面,选择“防病毒日志”选项卡,可以看到病毒过滤日志,服务为 HTTP,如图 6-138 所示。




图 6-137　验证测试

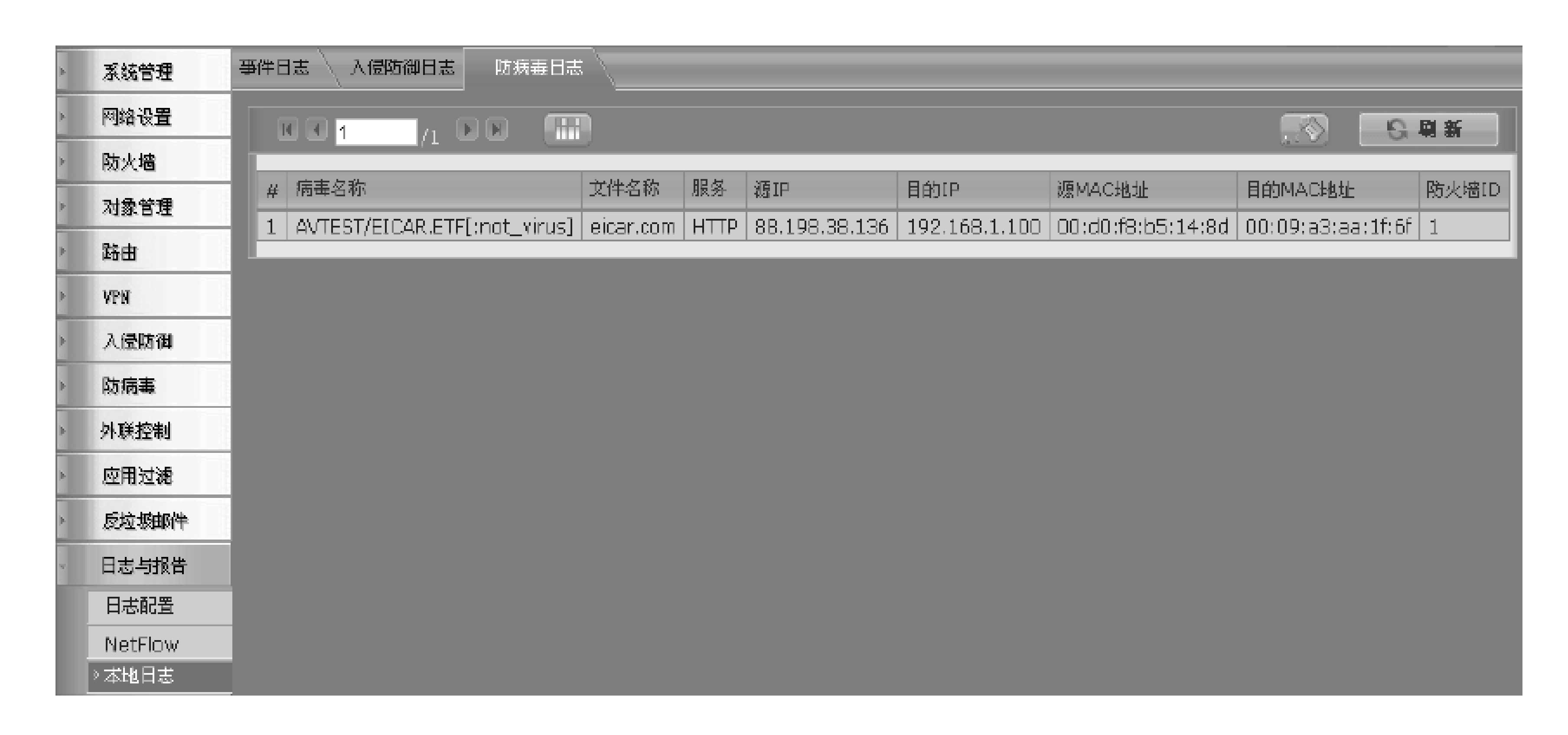



图 6-138　选择“防病毒日志”选项卡

## 【注意事项】

- 在实验中，请根据实际情况配置 USG 访问 Internet 的连接。
- 在实验中，强烈建议在客户端上安装反病毒软件，以免主机被病毒感染。
- 请勿将下载成功的病毒在网络中传播。

# 6.7　使用统一安全网关过滤邮件病毒

## 【实验名称】

使用统一安全网关过滤邮件病毒。

## 【实验目的】

使用(USG)统一安全网关过滤邮件(SMTP/POP3 流量)中的病毒。

## 【背景描述】

某企业为了提高网络的安全性，部署了一台 USG。但最近公司发现网络中有很多病

毒，而且这些病毒很多都是通过电子邮件进行传播。公司希望能够对员工发送和接收的邮件进行病毒扫描，防止发送和接收含有病毒的邮件。

## 【需求分析】

为了防止发送和接收带有病毒的邮件，提高网络安全性，可以在网络出口处进行邮件病毒检测，阻止含有病毒的邮件通过网关。

## 【实验拓扑】

如图 6-139 所示的网络拓扑，是某公司发现网络中有很多病毒，而且这些病毒很多都是通过电子邮件进行传播。公司希望能够对员工发送和接收的邮件进行病毒扫描，防止发送和接收含有病毒的邮件。企业为了提高网络的安全，购买了一台 RG-USG 统一安全网关，在网络出口处进行邮件病毒检测，阻止含有病毒的邮件通过网关，以实现网络的安全防范功能。

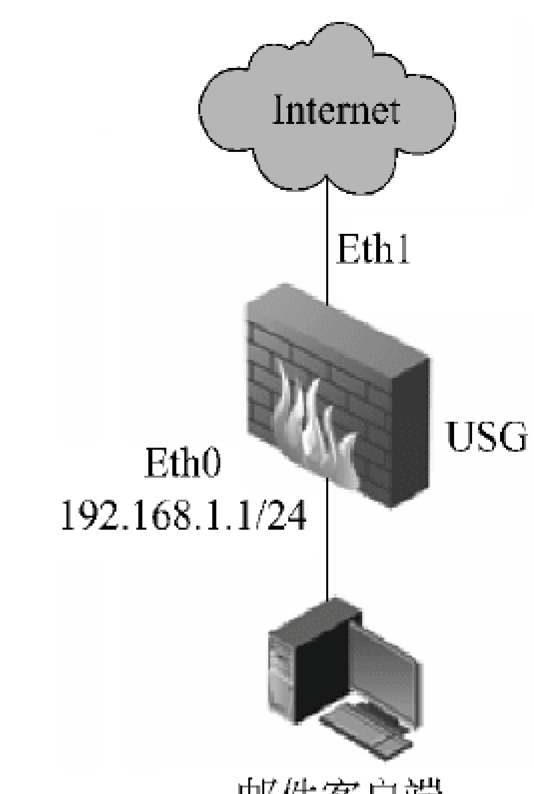



图 6-139 统一安全网关过滤邮件病毒网络拓扑图

## 【实验设备】

USG 连接到 Internet 的链路

USG 1 台

PC 1 台(安装邮件客户端)

## 【预备知识】

- 网络基础知识。
- USG 操作基础知识。

## 【实验原理】

USG 集成了网关病毒过滤功能，支持对邮件(SMTP/POP3 流量)进行病毒扫描，可以将含有病毒的邮件过滤掉。

## 【实验步骤】

### 1. 配置 USG接口的 IP地址

如图 6-140 所示，进入 USG 的配置页面，即“接口”页面。

单击 eth0 接口的“编辑”图标，为 eth0 接口配置 IP 地址及子网掩码，如图 6-141 所示。

单击 eth1 接口的“编辑”图标，为 eth1 接口配置 IP 地址及子网掩码。这里 eth1 接口作为连接到 Internet 的接口，请根据实际情况配置 eth1 接口的地址信息。

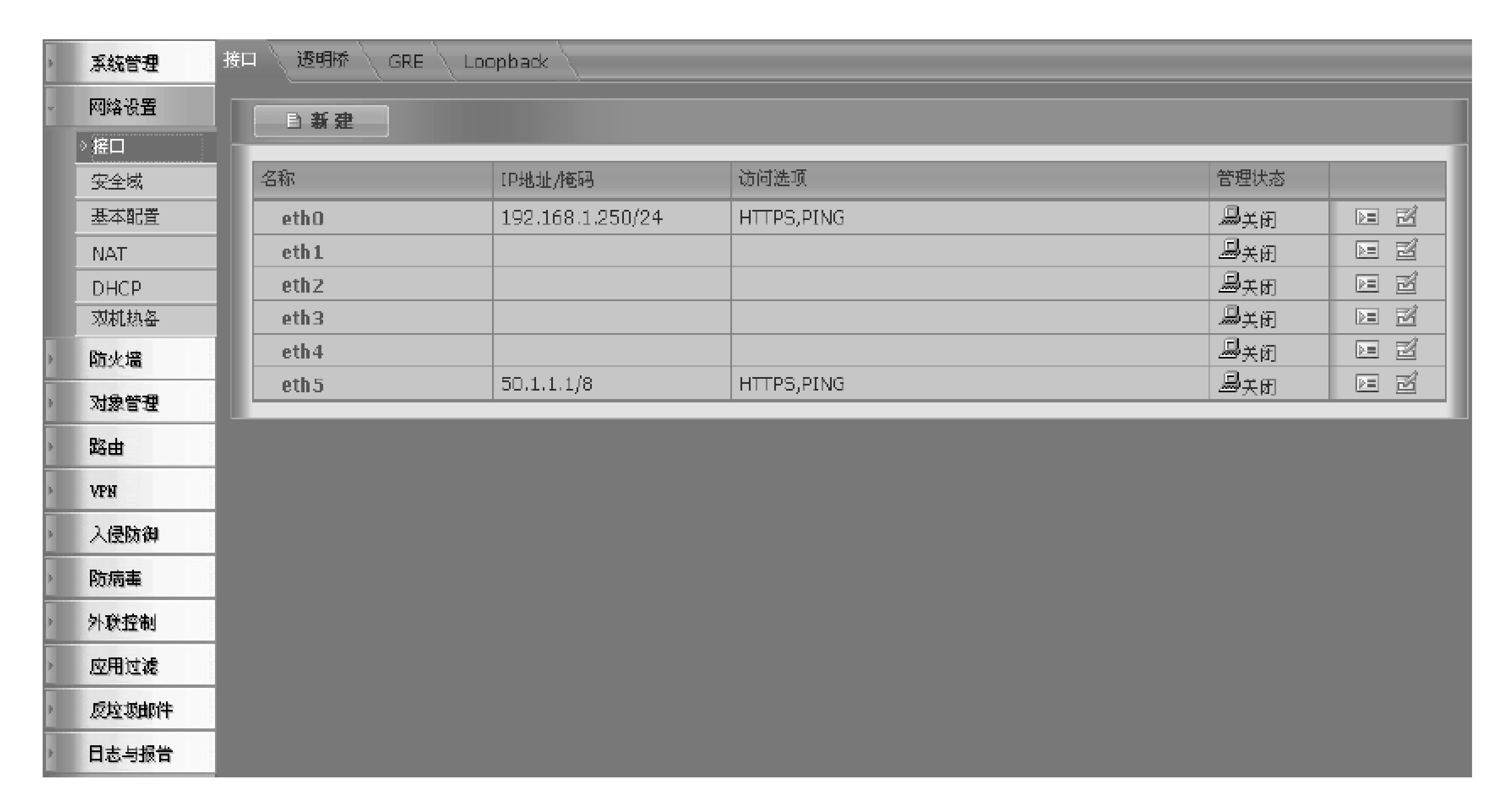



图 6-140　进入 USG 的配置页面




图 6-141　为 eth0 接口配置 IP 地址

## 2 配置 USG 的默认网关

进入 USG 的配置页面，即“基本配置”页面，在网关地址栏中，请根据实际情况配置访问 Internet 的默认网关地址，如图 6-142 所示。




图 6-142　进入 USG 的配置页面

### 3. 配置内部子网的地址对象

进入 USG 的配置页面，即“地址对象”页面，可以看到系统预定义了一个名为 any 的地址对象，它包括所有的地址 0.0.0.0/0，如图 6-143 所示。

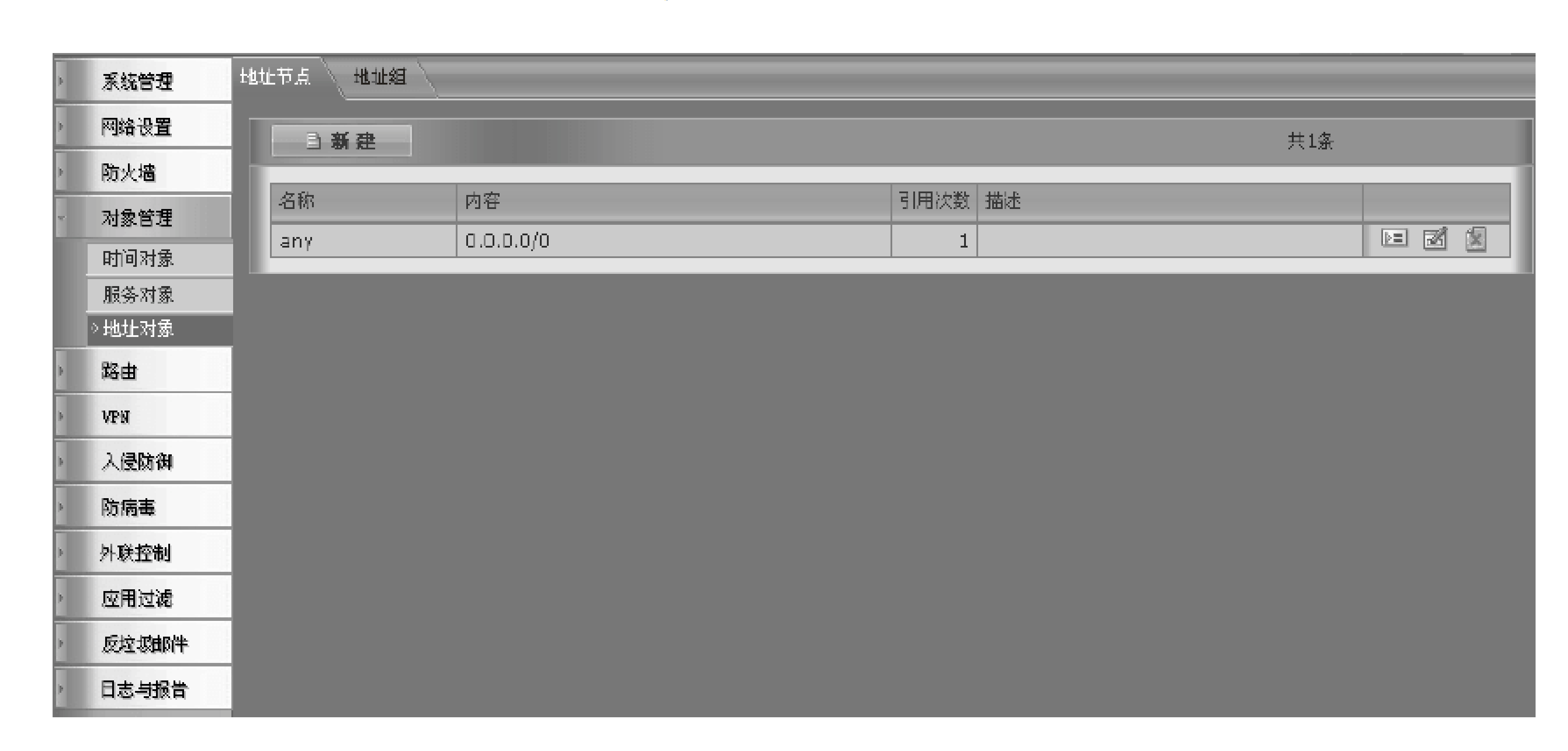



图 6-143　配置内部子网的地址对象

单击“新建”按钮创建地址对象，该地址对象包括公司内部子网 192.168.1.0/24，如图 6-144 所示。




图 6-144　创建地址对象

### 4. 配置 NAT

进入 USG 的配置页面，即 NAT 页面，单击“新建”按钮创建 NAT 规则。

NAT 规则中的源地址选择之前创建的 inside 地址对象，目标地址使用 any 地址对象，服务使用 any 服务对象，出接口为连接 Internet 的 eth1 接口，转换后源地址为“出接口地址”，即 eth1 接口的地址，如图 6-145 和图 6-146 所示。

### 5. 配置防病毒

进入 USG 配置页面，即“文件扫描列表”页面，选择需要进行病毒扫描的文件类型，如图 6-147 所示。




图 6-145　配置 NAT 规则(1)




图 6-146　配置 NAT 规则(2)




图 6-147　进入 USG 配置页面

## 6. 配置安全防护表

进入 USG 配置页面，即“安全策略”页面，选择“安全防护表”选项卡，如图 6-148 所示。

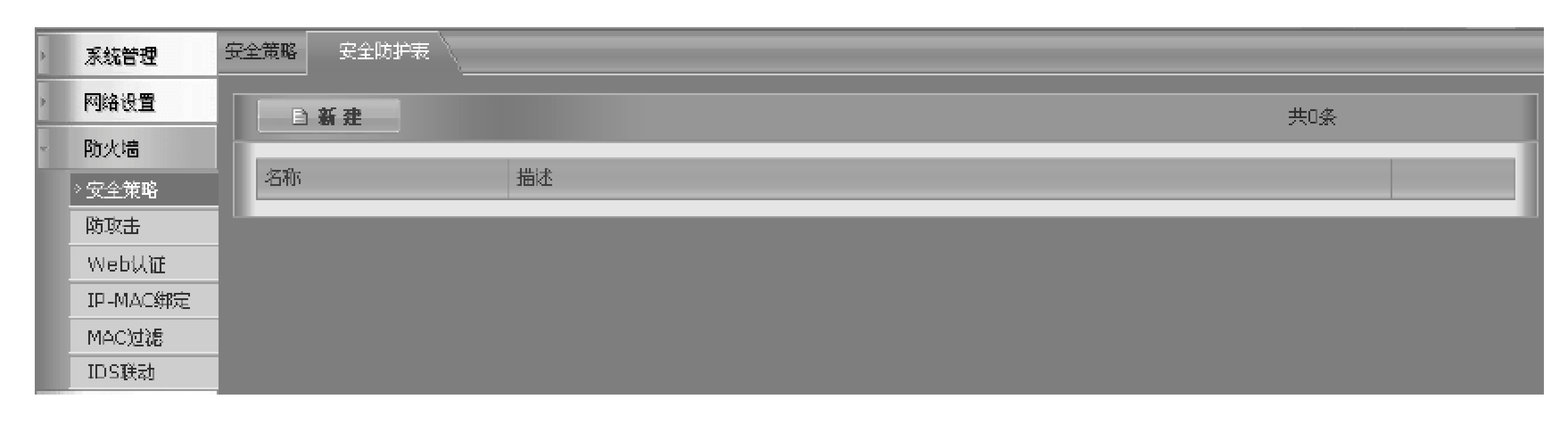



图 6-148　配置安全防护表

单击“新建”按钮创建安全防护表。为安全防护表配置名称，选择并展开“防病毒”选项，选择对 IMAP、POP3 和 SMTP 流量进行文件扫描，如图 6-149 所示。




图 6-149　创建安全防护表

仍然在该防护表中选择并展开“日志”选项，选择本地日志中的“防病毒”选项，记录本地日志，如图 6-150 和图 6-151 所示。

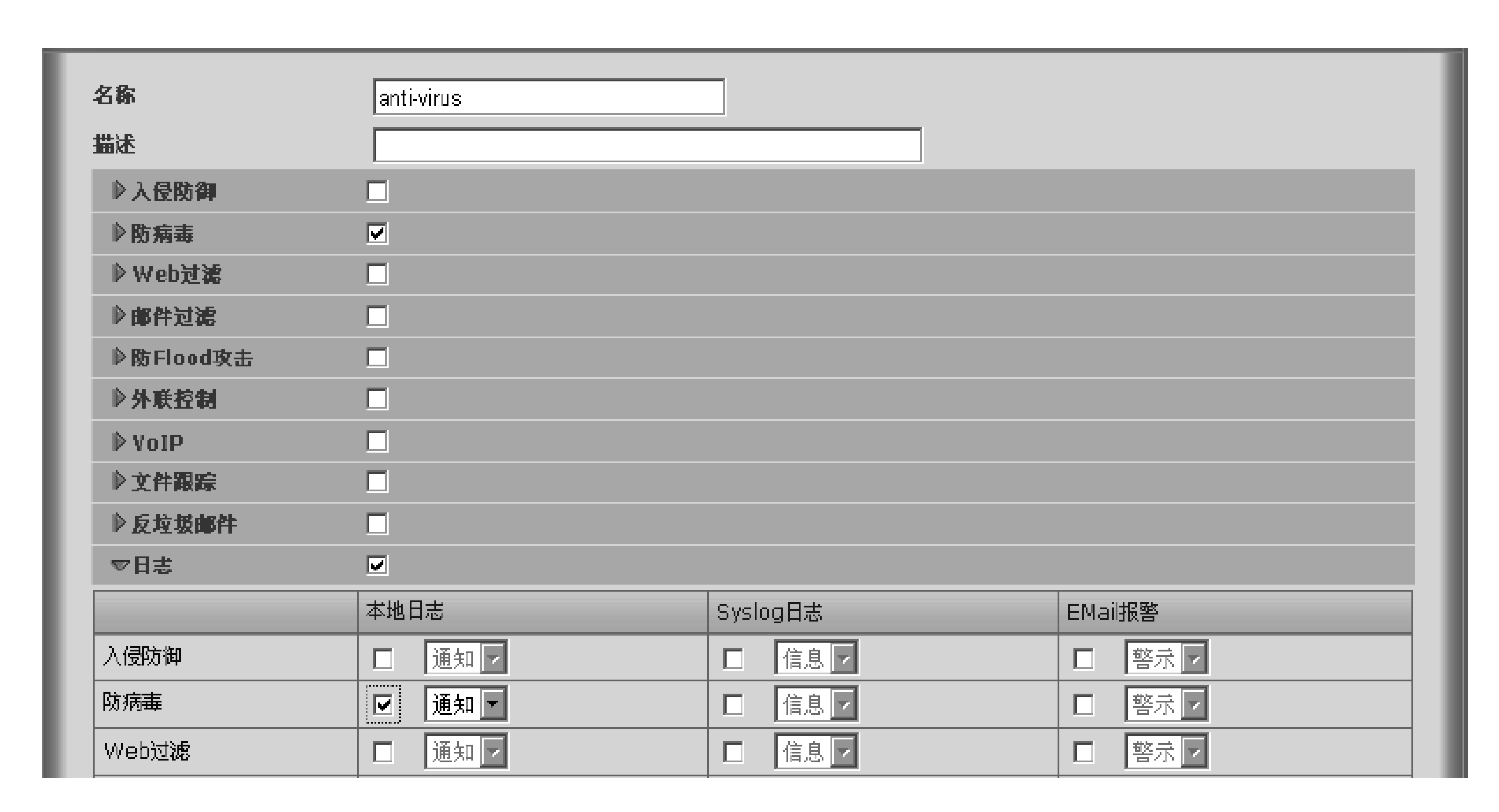



图 6-150　选择本地日志中的“防病毒”选项

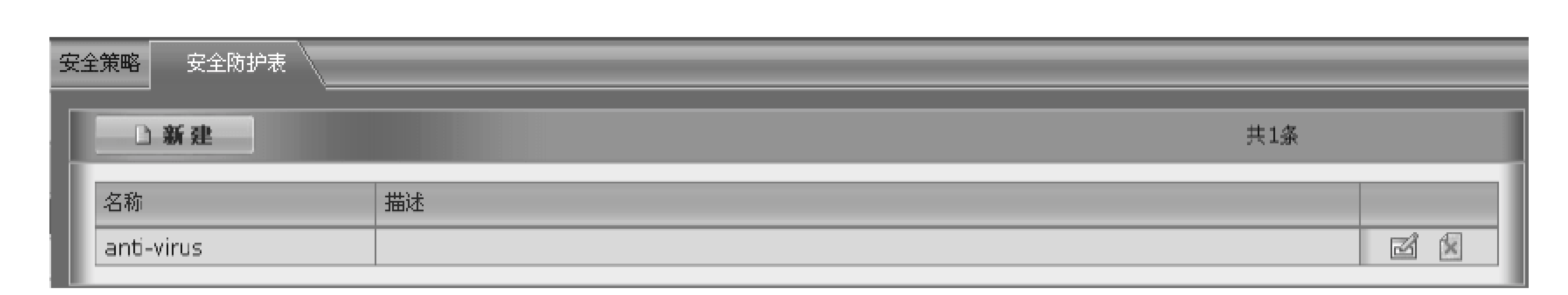



图 6-151　记录本地日志

## 7. 配置安全策略

进入 USG 配置页面，即“安全策略”页面，如图 6-152 所示。

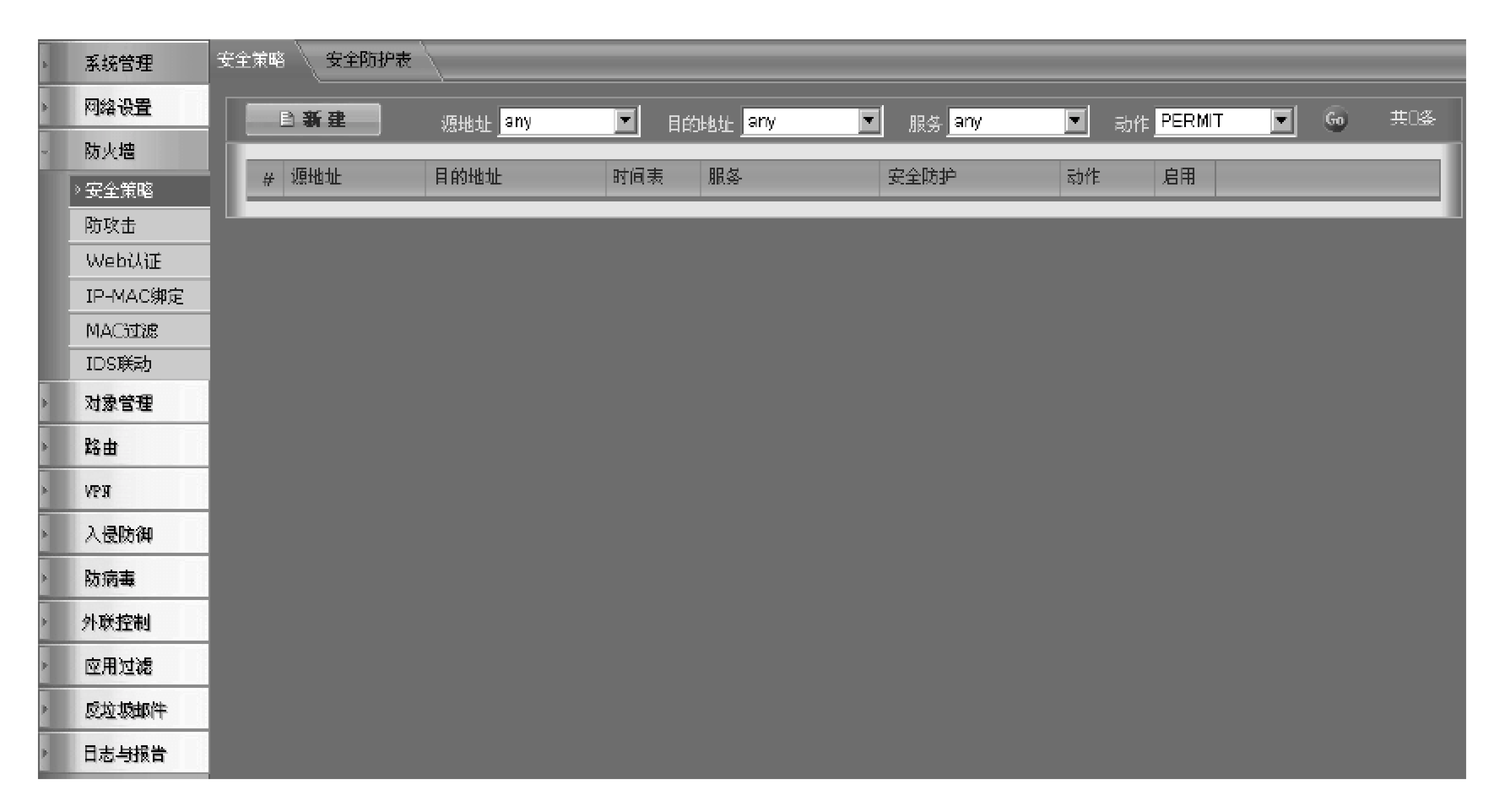



图 6-152　进入 USG 配置页面

单击“新建”按钮创建安全策略。在安全策略中源接口为 eth0 接口；源地址为 inside 地址对象；目的接口为 eth1 接口；目的地址为 any 地址对象；服务为 any 服务对象；时间表为 always 地址对象，代表任何时间；动作为 PERMIT 允许；在“安全防护”下拉列表中选择之前创建的安全防护表，如图 6-153 所示。




图 6-153　创建安全策略

创建完安全策略后，需要选择“启用”选项来使该规则生效，如图 6-154 所示。




图 6-154　启用安全策略

### 8. 验证测试

在内部 PC 上使用邮件客户端(例如 Outlook Express)发送合法的、不含有病毒的邮件,可以成功发送,并且收件人可以成功接收到邮件,如图 6-155 所示。




图 6-155　验证测试

然后再使用邮件客户端发送带有病毒样本附件(acid.zip)的邮件,此时邮件客户端提示无法发送邮件,如图 6-156 所示。

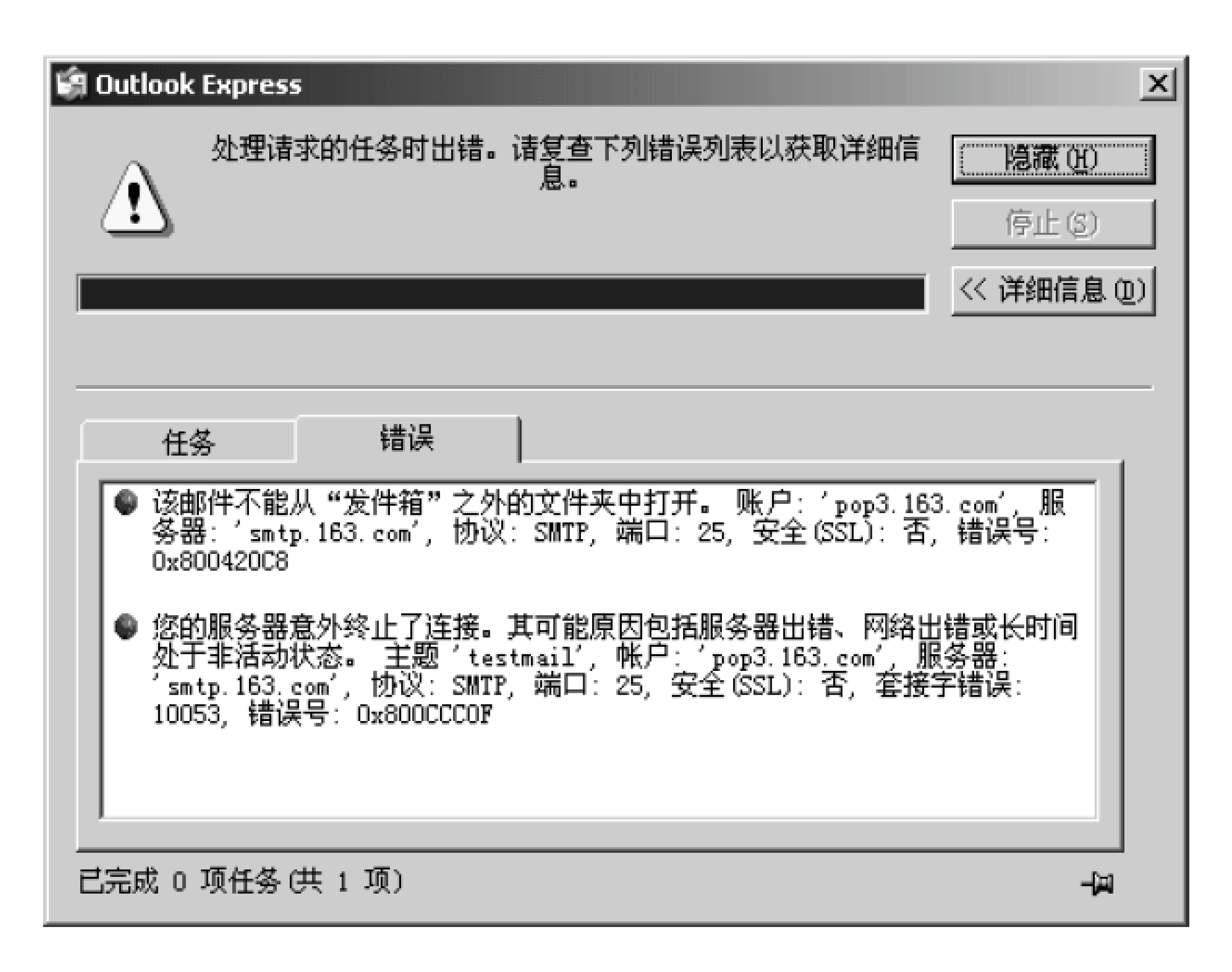



图 6-156　邮件客户端提示无法发送邮件

进入 USG 配置页面,即"本地日志"页面,选择"防病毒日志"选项卡,可以看到病毒过滤日志,服务为 SMTP,如图 6-157 所示。

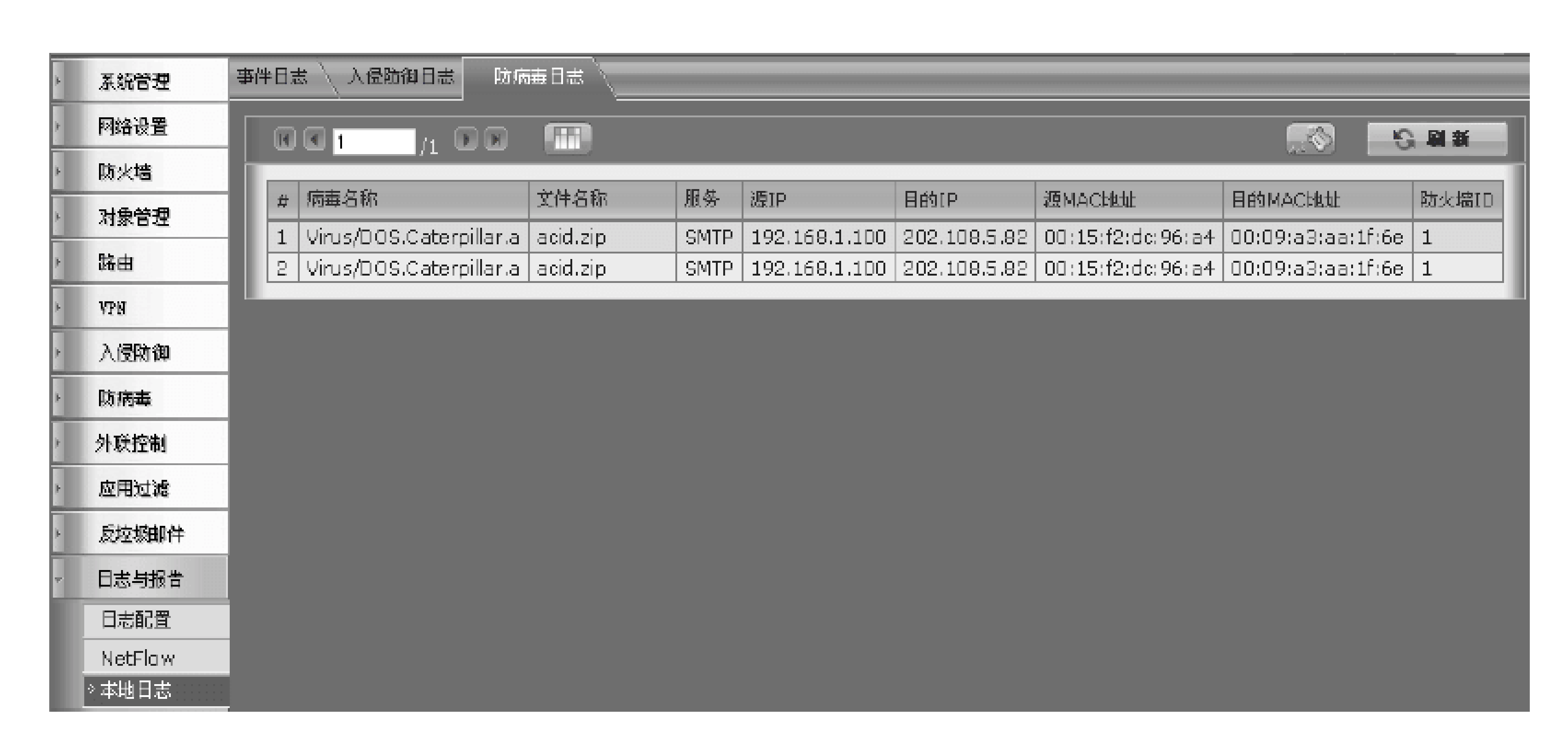



图 6-157　进入 USG 配置页面

## 【注意事项】

- 在实验中,请根据实际情况配置 USG 访问 Internet 的连接。
- 在实验中,强烈建议在客户端上安装反病毒软件,以免主机被病毒感染。
- 请勿将病毒样本在网络中传播。
- 由于 Internet 中的很多邮件服务器也都对邮件进行病毒扫描与过滤,所以为了使该实验效果更加明显和直观,本实验使用 USG 检测内部向外部发送的邮件。当使用 USG 检测外部向内部发送的邮件时,有可能在 USG 上看不到记录日志,这是因为 Internet 中的邮件服务器已经将邮件中的病毒过滤掉了。

# 6.8　配置邮件大小过滤

## 【实验名称】

配置邮件大小过滤。

## 【实验目的】

使用(USG)统一安全网关根据邮件大小进行邮件过滤。

## 【背景描述】

某企业为了提高网络的安全性,部署了一台 USG。但最近公司发现许多员工在发送邮件时,经常附带容量很大的附件,使整个邮件的容量变得很大,严重影响了邮件系统的正常工作。公司希望能够对员工向外部发送的邮件大小进行限制,不允许员工发送大小超过 1MB 的邮件。

## 【需求分析】

为了实现对邮件大小进行监控和限制,可以使用 USG 的邮件过滤功能,只允许用户

发送小于许可容量大小的邮件。

## 【实验拓扑】

如图 6-158 所示的网络拓扑，是企业为了提高网络的安全，购买的一台 RG-USG 统一安全网关。网络管理员发现最近公司发现许多员工在发送邮件时，经常附带容量很大的附件，使整个邮件的容量变得很大，严重影响了邮件系统的正常工作。公司希望能够对员工向外部发送的邮件大小进行限制，不允许员工发送大小超过 1M 的邮件，现在需要登录到 USG 并对其进行基本配置，使用 USG 的邮件过滤功能，只允许用户发送小于许可容量大小的邮件。

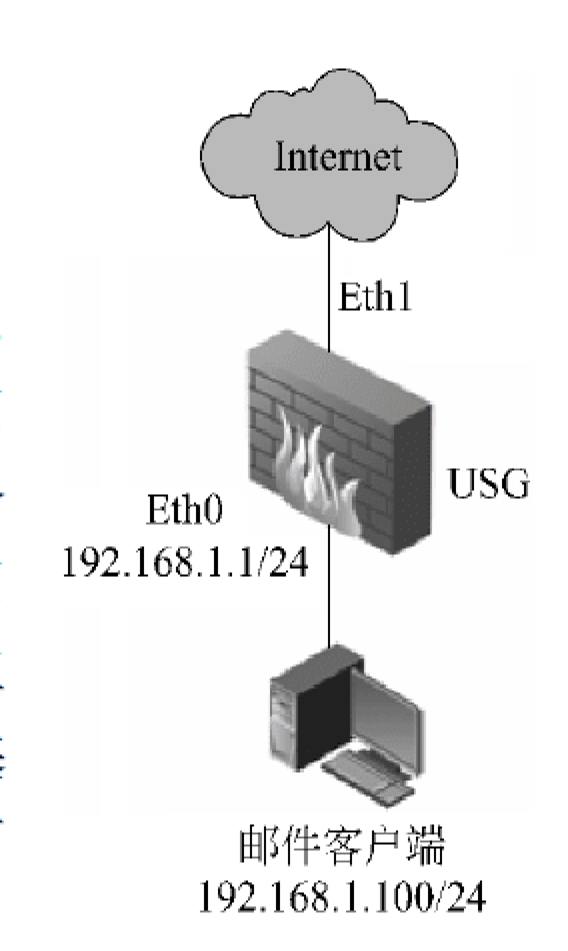



图 6-158　配置邮件大小过滤网络拓扑图

## 【实验设备】

USG 连接到 Internet 的链路
USG　1 台
PC　　1 台(安装邮件客户端)

## 【预备知识】

- 网络基础知识。
- USG 操作基础知识。

## 【实验原理】

USG 支持对邮件进行过滤。USG 不仅可以对邮件的发件人、主题等进行过滤，还可以限制邮件的大小。

## 【实验步骤】

### 1. 配置 USG 接口的 IP 地址

如图 6-159 所示，进入 USG 的配置页面，即“接口”页面。

单击 eth0 接口的“编辑”图标，为 eth0 接口配置 IP 地址及子网掩码，如图 6-160 所示。

单击 eth1 接口的“编辑”图标，为 eth1 接口配置 IP 地址及子网掩码。这里 eth1 接口作为连接到 Internet 的接口，请根据实际情况配置 eth1 接口的地址信息。

### 2. 配置 USG 的默认网关

进入 USG 的配置页面，即“基本配置”页面，在网关地址栏中，请根据实际情况配置访问 Internet 的默认网关地址，如图 6-161 所示。

### 3. 配置内部子网的地址对象

进入 USG 的配置页面，即“地址对象”页面，可以看到系统预定义了一个名为 any 的

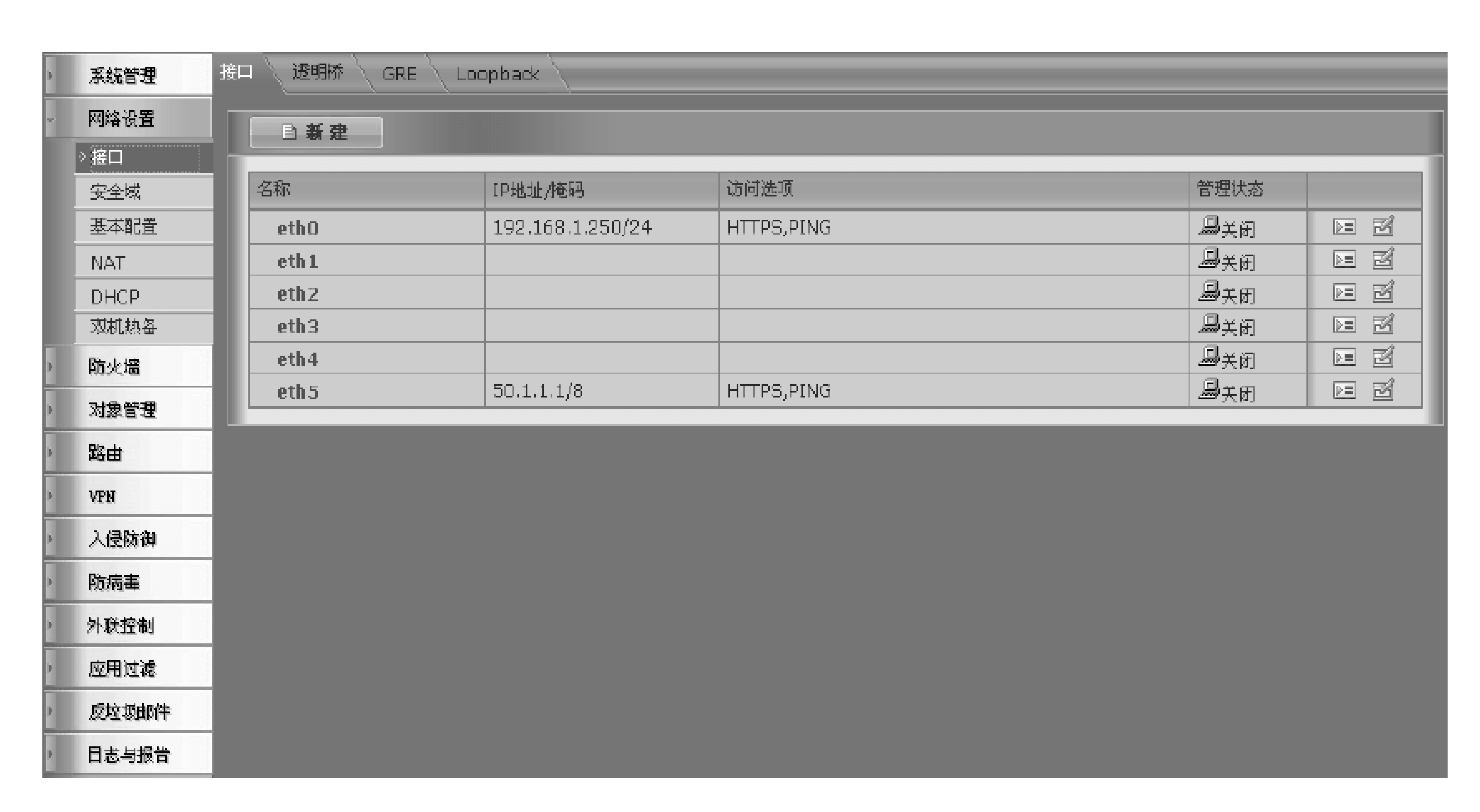



图 6-159　进入 USG 的配置页面(1)

图 6-160　为 eth0 接口配置 IP 地址




图 6-161　进入 USG 的配置页面(2)

地址对象,它包括所有的地址 0.0.0.0/0,如图 6-162 所示。

单击“新建”按钮创建地址对象,该地址对象包括公司内部子网 192.168.1.0/24,如图 6-163 所示。

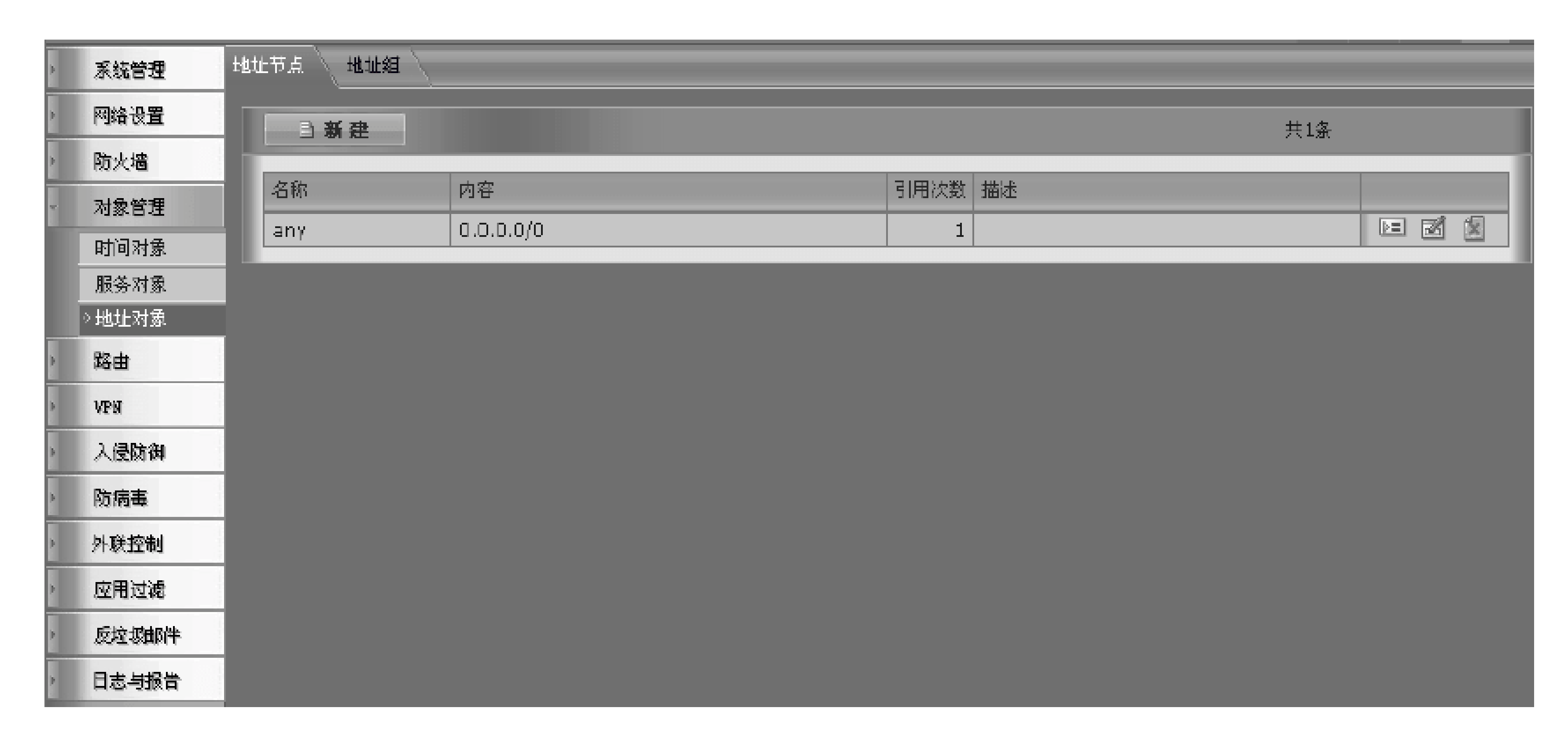



图 6-162　配置内部子网的地址对象




图 6-163　创建地址对象

## 4. 配置 NAT

进入 USG 的配置页面，即 NAT 页面，单击“新建”按钮创建 NAT 规则。

NAT 规则中的源地址选择之前创建的 inside 地址对象，目标地址使用 any 地址对象，服务使用 any 服务对象，出接口为连接 Internet 的 eth1 接口，转换后源地址为“出接口地址”，即 eth1 接口的地址，如图 6-164 和图 6-165 所示。




图 6-164　配置 NAT(1)




图 6-165　配置 NAT(2)

## 5. 配置邮件过滤

进入 USG 配置页面,即“邮件过滤”页面,选择“邮件大小过滤”选项卡,将邮件大小限制为 1MB,如图 6-166 所示。




图 6-166　配置邮件过滤

## 6. 配置安全防护表

进入 USG 配置页面,即“安全策略”页面,选择“安全防护表”选项卡,如图 6-167 所示。




图 6-167　配置安全防护表

单击“新建”按钮创建安全防护表。为安全防护表配置名称,选择并展开“邮件过滤”选项,选择“邮件大小屏蔽”选项,如图 6-168 所示。




图 6-168　创建安全防护表

仍然在该防护表中选择并展开“日志”选项，选择本地日志中的“邮件过滤”选项，记录本地日志，如图 6-169 和图 6-170 所示。

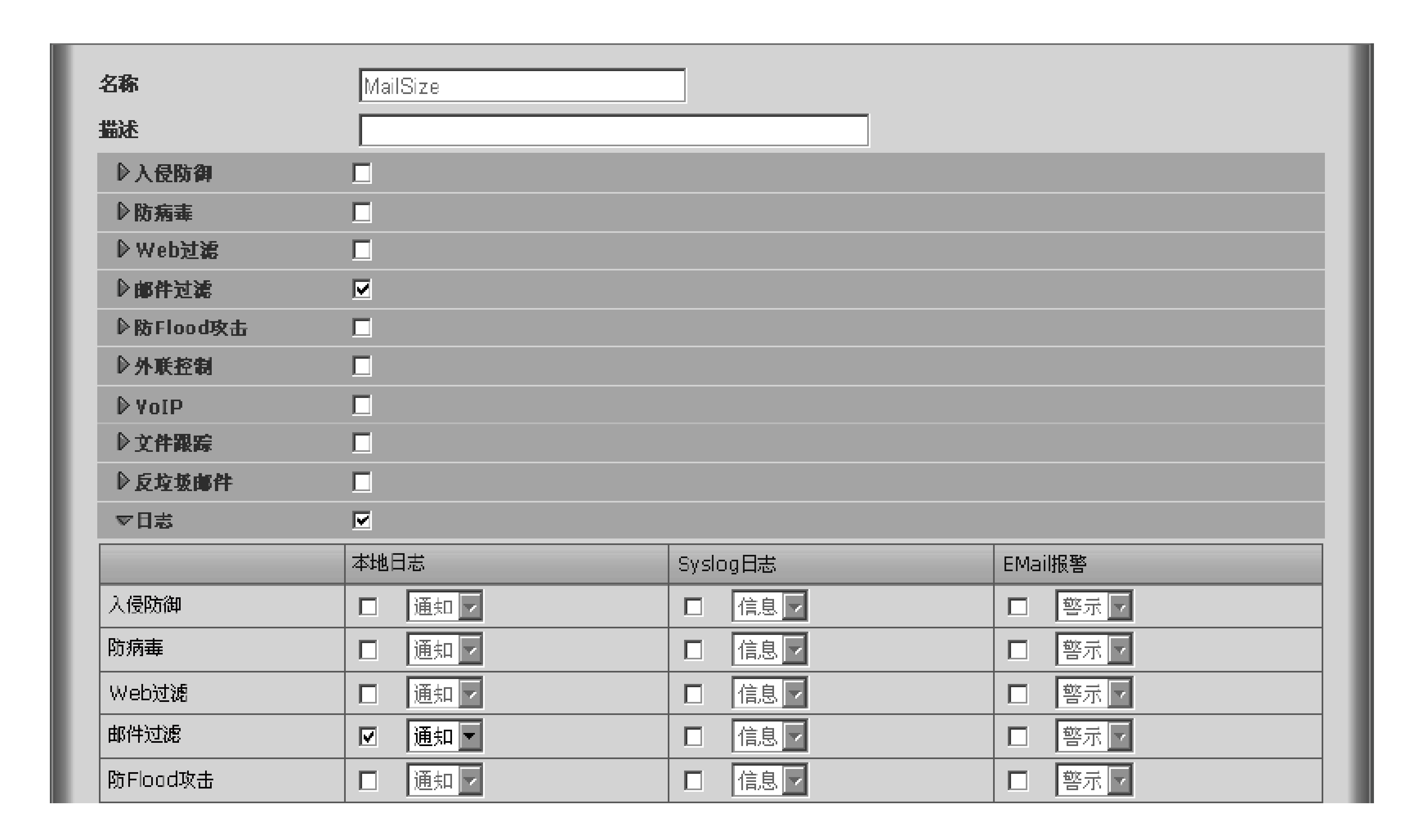



图 6-169　选择本地日志中的“邮件过滤”选项

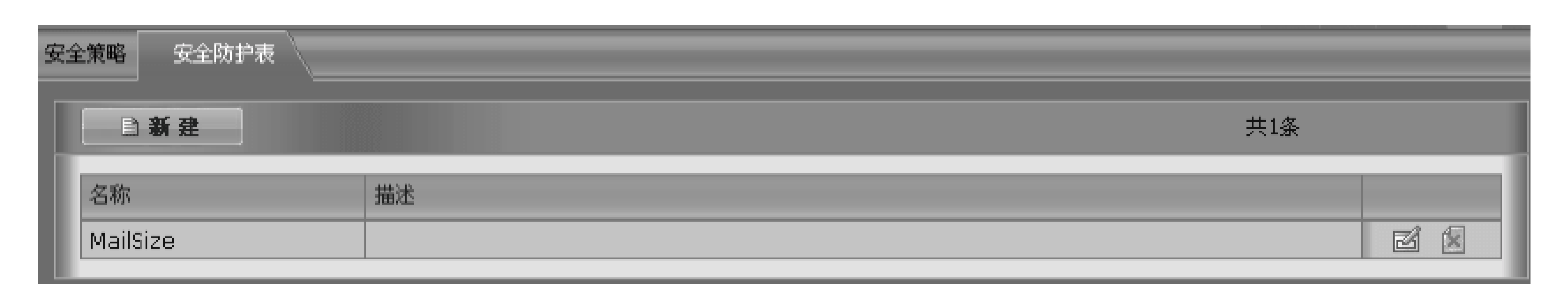



图 6-170　记录本地日志

## 7. 配置安全策略

进入 USG 配置页面，即“安全策略”页面，如图 6-171 所示。

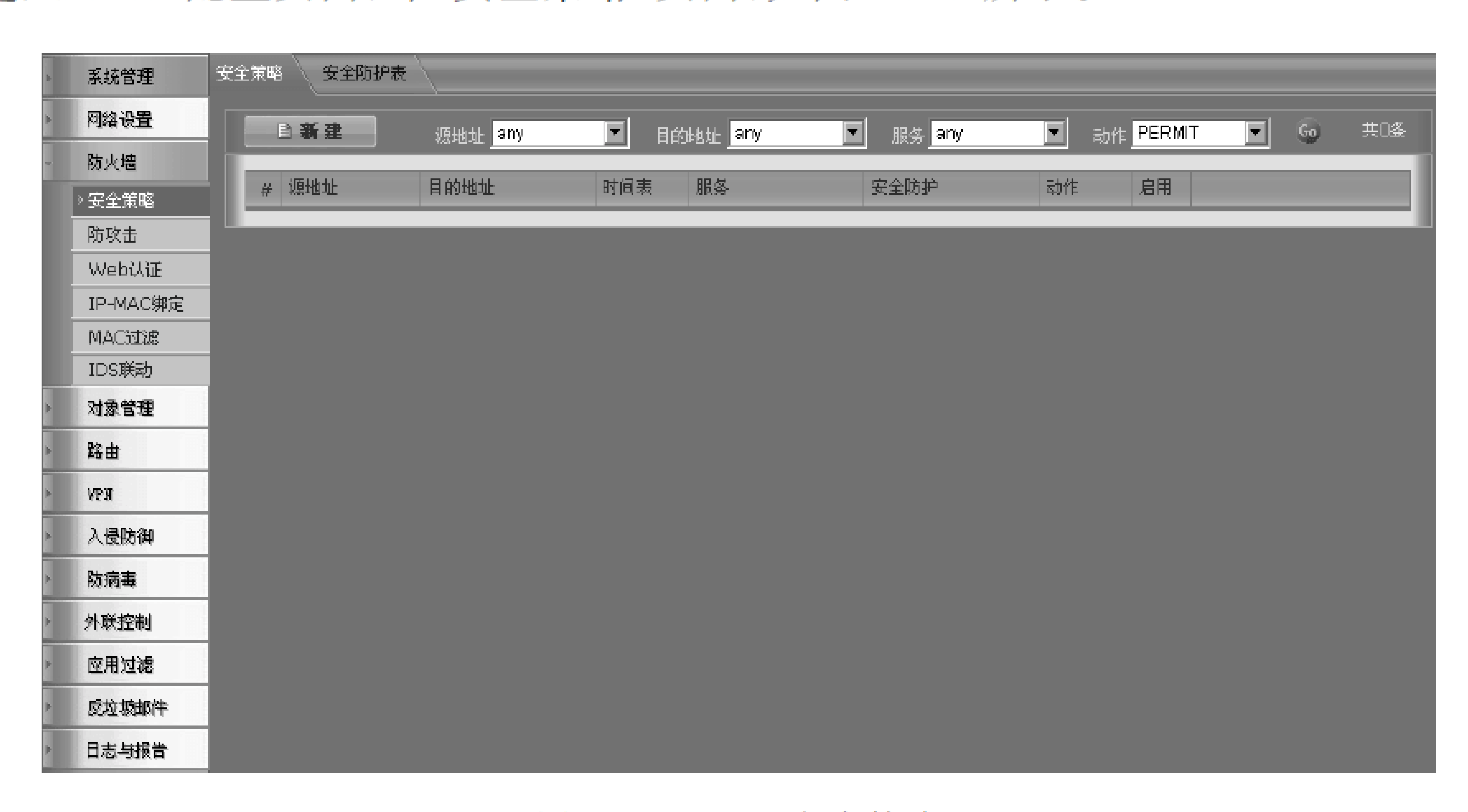



图 6-171　配置安全策略

单击“新建”按钮创建安全策略。在安全策略中源接口为 eth0 接口；源地址为 inside 地址对象；目的接口为 eth1 接口；目的地址为 any 地址对象；服务为 any 服务对象；时间

表为 always 地址对象,代表任何时间;动作为 PERMIT 允许;在“安全防护”下拉列表中选择之前创建的安全防护表 MailSize,如图 6-172 所示。




图 6-172 创建安全策略

创建完安全策略后,需要选择“启用”选项使该规则生效,如图 6-173 所示。




图 6-173 启用安全策略

## 8. 验证测试

首先在客户端上使用邮件客户端(例如 Outlook Express)发送小于 1MB 的邮件,可以成功发送,如图 6-174 所示。

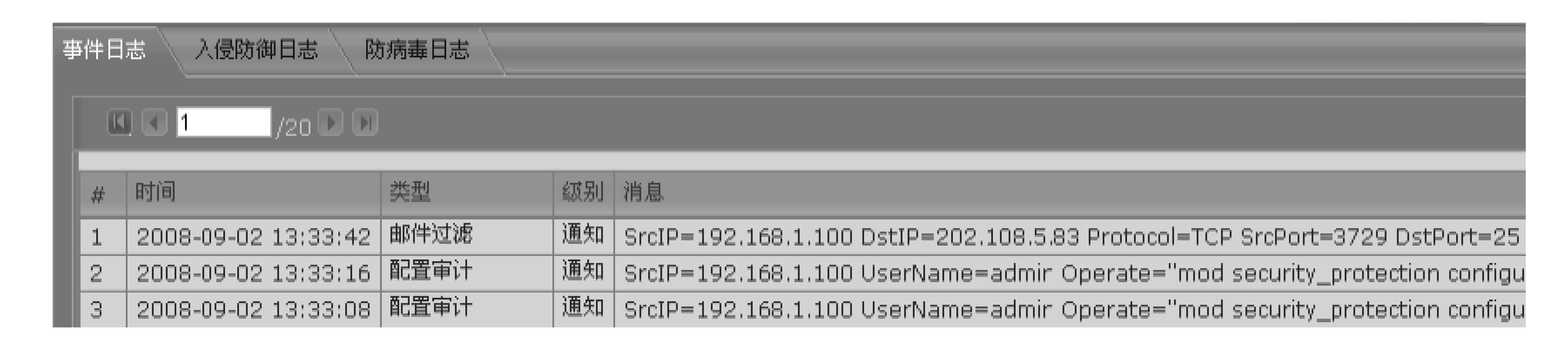



图 6-174 验证测试(1)

然后再发送一个大于 1MB 的含附件的邮件,不能成功发送。说明 USG 的邮件过滤功能生效,将超过 1MB 的邮件过滤掉了,如图 6-175 所示。

进入 USG 配置页面,即“本地日志”页面,选择“事件日志”选项卡,可以看到由于邮件过大,导致邮件被过滤的日志。日志中显示类型为邮件过滤,原因是 mail size is too long。

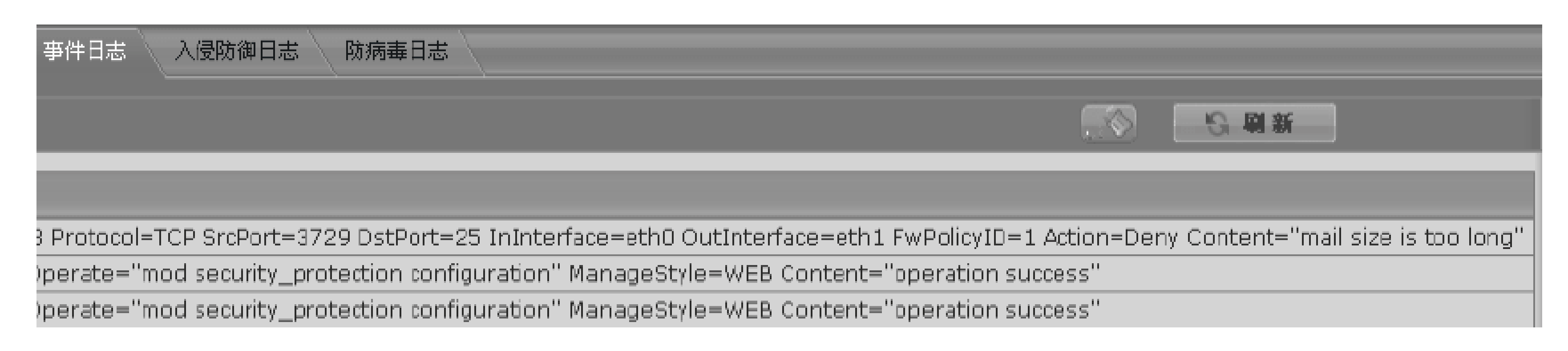

事件日志 入侵防御日志 防病毒日志
刷新
3 Protocol=TCP SrcPort=3729 DstPort=25 InInterface=eth0 OutInterface=eth1 FwPolicyID=1 Action=Deny Content="mail size is too long"
)perate="mod security_protection configuration" ManageStyle=WEB Content="operation success"
)perate="mod security_protection configuration" ManageStyle=WEB Content="operation success"

图 6-175 验证测试(2)

### 【注意事项】

- 在实验中,请根据实际情况配置 USG 访问 Internet 的连接。
- 邮件过滤是针对 SMTP 的流量(通常使用邮件客户端发送的邮件)进行过滤,对于使用 Web 邮箱(即 HTTP)的邮件无效。

## 6.9 使用统一安全网关实现入侵防御

### 【实验名称】

使用统一安全网关实现入侵防御。

### 【实验目的】

利用 USG(统一安全网关)的入侵防御(IPS)功能,检测并阻止网络攻击。

### 【背景描述】

某公司使用 USG 作为网络出口设备连接到 Internet,并且公司内部有一台对外提供服务的 Web 服务器。最近网络管理员发现 Internet 中有人向 Web 服务器发起攻击,影响了服务器的正常运行。公司希望阻止病毒入侵服务器。

### 【需求分析】

要防止来自外部网络的攻击,可以使用 USG 的入侵防御功能。

### 【实验拓扑】

如图 6-176 所示的网络拓扑,是企业为了提高网络的安全,购买了一台 RG-USG 统一安全网关,公司使用 USG 作为网络出口设备连接到 Internet,并且公司内部有一台对外提供服务的 Web 服务器。最近网络管理员发现

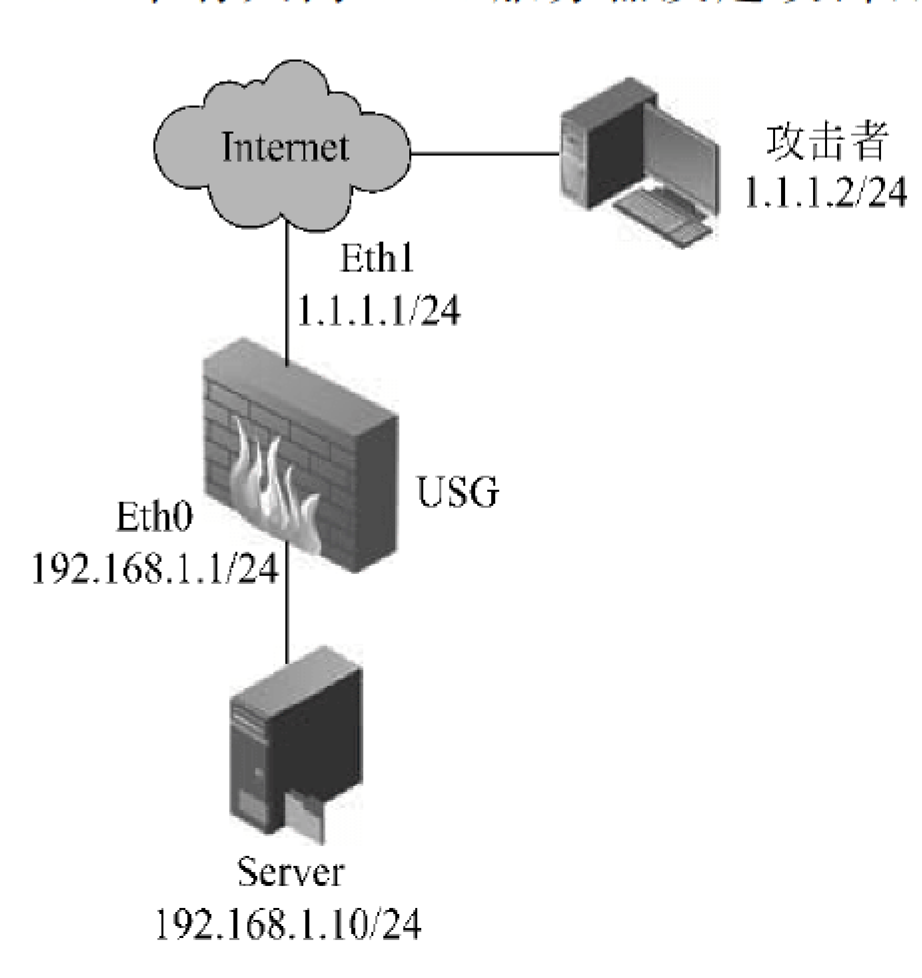



图 6-176 统一安全网关实现入侵防御网络拓扑图

Internet 中有人向 Web 服务器发起攻击，影响了服务器的正常运行。现在需要登录到 USG 并对其进行基本配置，防止来自外部网络的攻击，可以使用 USG 的入侵防御功能，实现网络的安全防范功能。

## 【实验设备】

| | |
|---|---|
| USG | 1 台 |
| Windows 2000 Server | 1 台(未安装 Service Packet，模拟被攻击机，并且安装 IIS 服务) |
| 缓冲区溢出攻击工具 | imap_exp. exe |
| IIS 攻击工具 | GUI_Unicode. exe |

## 【预备知识】

- 网络基础知识。
- USG 操作基础知识。

## 【实验原理】

USG 的入侵防御(IPS)功能可以对大量的入侵攻击进行检测和阻断。当 USG 发现数据流中存在恶意代码，或者具有攻击特征时，会对攻击进行报警，并采取相应的阻断措施。

## 【实验步骤】

### 1. 配置 USG 接口的 IP 地址

如图 6-177 所示，进入 USG 的配置页面，即“接口”页面。




图 6-177　进入 USG 的配置页面

单击 eth0 接口的“编辑”图标，为 eth0 接口配置 IP 地址及子网掩码，如图 6-178 所示。

单击 eth1 接口的“编辑”图标，为 eth1 接口配置 IP 地址及子网掩码，如图 6-179 所示。

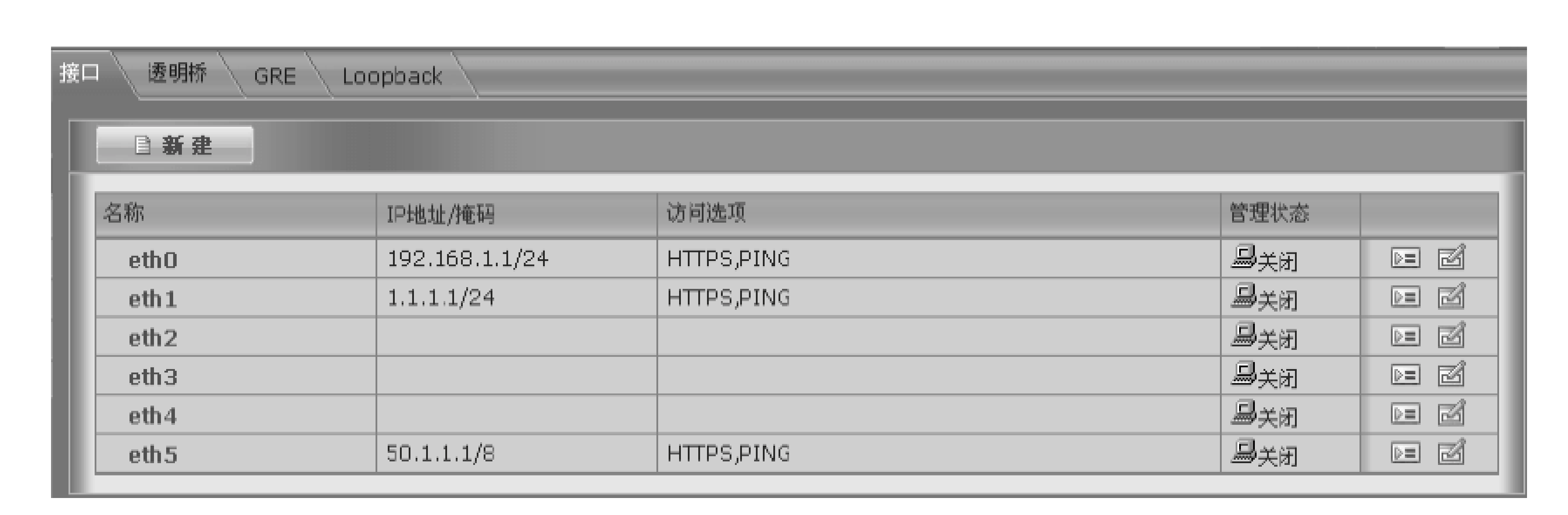



图 6-178 为 eth0 接口配置 IP 地址




图 6-179 为 eth1 接口配置 IP 地址

接口配置 IP 地址后的状态如图 6-180 所示。




| 名称 | IP地址/掩码 | 访问选项 | 管理状态 | |
|---|---|---|---|---|
| eth0 | 192.168.1.1/24 | HTTPS,PING | 关闭 | |
| eth1 | 1.1.1.1/24 | HTTPS,PING | 关闭 | |
| eth2 | | | 关闭 | |
| eth3 | | | 关闭 | |
| eth4 | | | 关闭 | |
| eth5 | 50.1.1.1/8 | HTTPS,PING | 关闭 | |

图 6-180 接口配置 IP 地址后的状态

## 2 配置静态 NAT 转换

为了使 Internet 中的用户可以访问内部的 FTP 服务器，需要在 USG 上配置静态 NAT 转换，将服务器发布到 Internet 中，如图 6-181 所示。




图 6-181　配置静态 NAT 转换

进入 USG 配置页面,即 NAT 页面,选择“静态地址转换”单选按钮。

单击“新建”按钮创建静态地址转换规则。规则中的“外部地址”为服务器对外发布的地址;“内部地址”为服务器实际的内部地址;“外部接口”为连接 Internet 的 eth1 接口,如图 6-182 所示。




图 6-182　创建静态地址转换规则

## 3. 配置安全防护表

进入 USG 配置页面,即“安全策略”页面,选择“安全防护表”选项卡,如图 6-183 所示。




图 6-183　配置安全防护表

单击“新建”按钮创建安全防护表。为安全防护表配置名称,选择并展开“入侵防御”选项,选择 All 事件集,表示 USG 将为流量匹配所有的事件(特征)。然后选择并展开“日志”选项,选择本地日志中的“入侵防御”选项,记录本地日志,如图 6-184 和图 6-185 所示。

## 4. 配置安全策略

进入 USG 配置页面,即“地址对象”页面,配置包含内部服务器的地址对象,如图 6-186 所示。




图 6-184　创建安全防护表

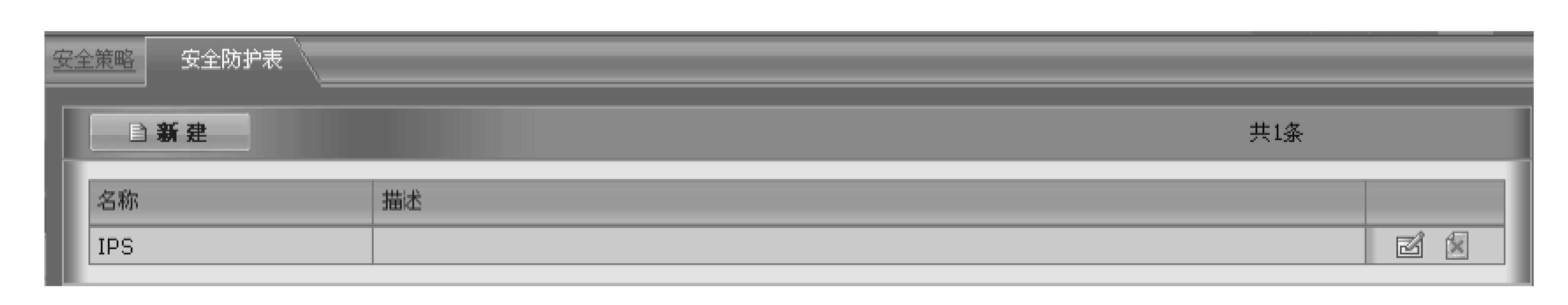



图 6-185　记录本地日志

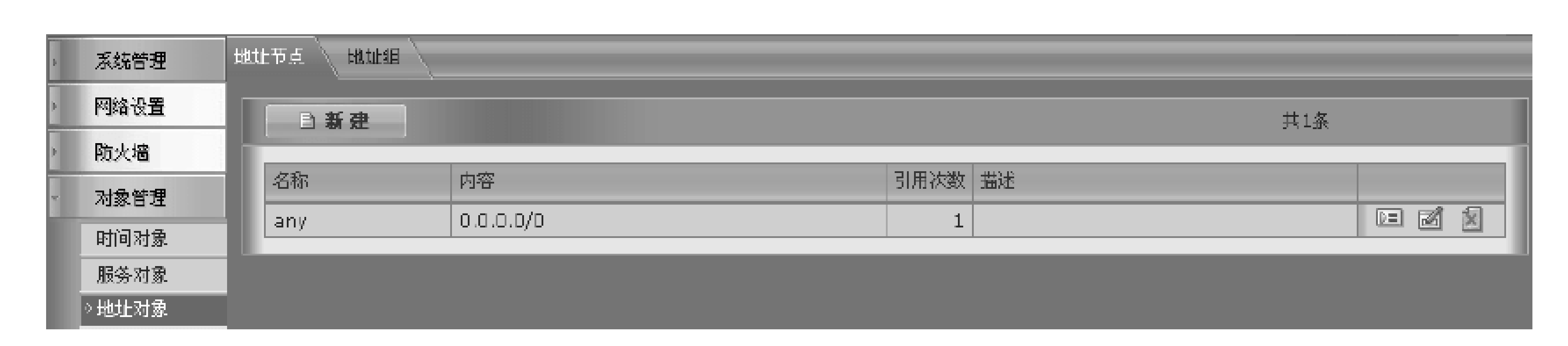



图 6-186　配置安全策略

单击“新建”按钮创建地址对象，地址为服务器的内部地址 192.168.1.10，如图 6-187 所示。

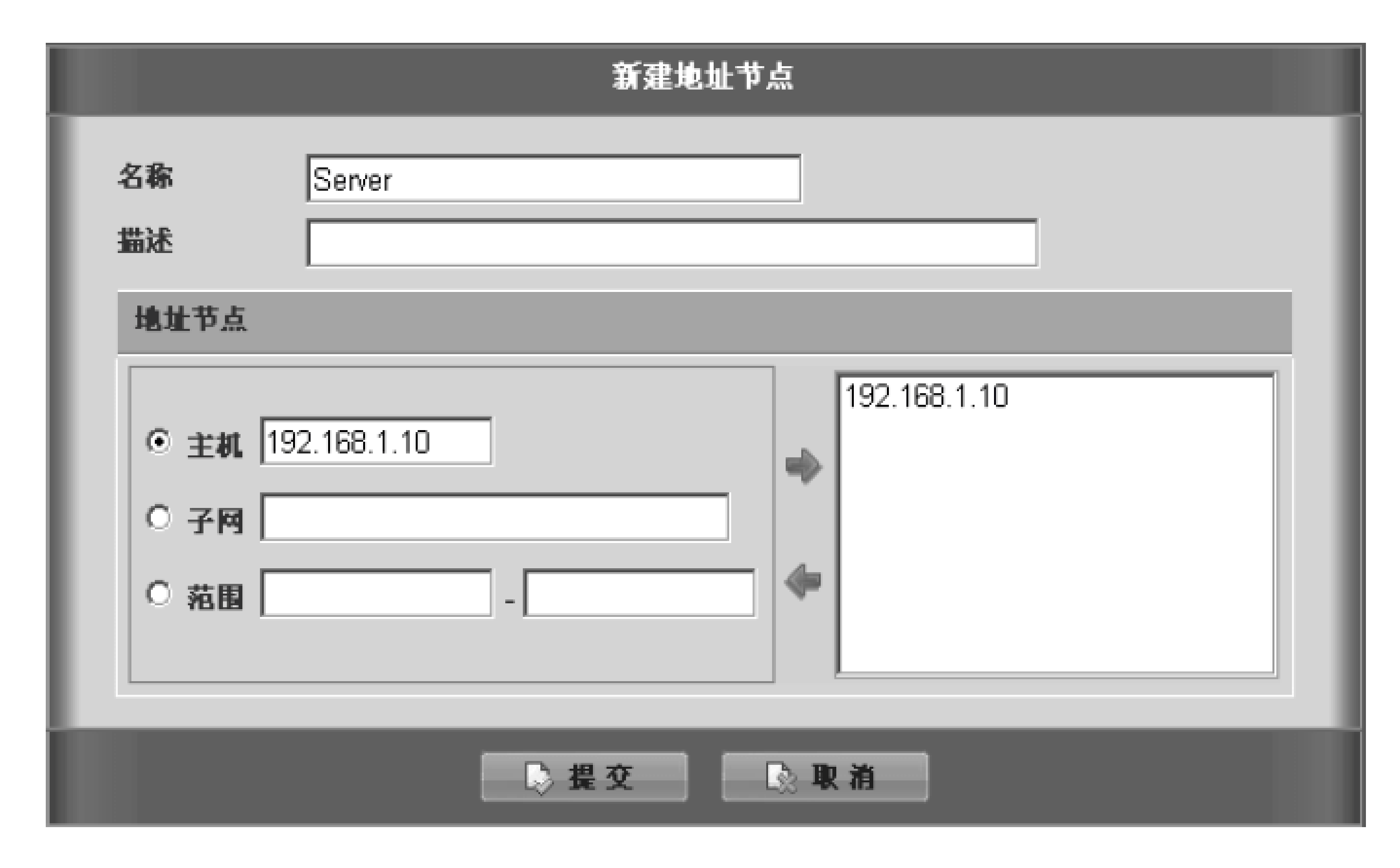



图 6-187　创建地址对象

进入 USG 配置页面，即“安全策略”页面，配置允许外部访问内部服务器的安全策略。

单击“新建”按钮创建安全策略。在安全策略中源接口为 eth1 接口；源地址为 any 地址对象；目的接口为 eth0 接口；目的地址为 Server 地址对象；服务为 any 服务对象；时间表为 always 地址对象，代表任何时间；动作为 PERMIT 允许；在“安全防护”下拉列表中选择刚刚创建的安全防护表 IPS，如图 6-188 所示。




图 6-188　创建安全策略

创建完安全策略后，需要选择“启用”选项使该规则生效，如图 6-189 所示。




图 6-189　启用安全策略

## 5. 验证测试

在模拟内网的内部 PC 上安装 Windows IIS 组件，并建立 Web 站点。在模拟外网的外部 PC 上使用 ping 测试命令测试访问服务器的连通性，可以 ping 通，如图 6-190 所示。

## 6. 实施缓冲区溢出攻击

在服务器（被攻击机）的命令行界面中运行 nc.exe，此时服务器的 389(LDAP)端口将被打开，如图 6-191 和图 6-192 所示。

```
C:\WINDOWS\system32\cmd.exe
Microsoft Windows XP [版本 5.1.2600]
(C) 版权所有 1985-2001 Microsoft Corp.

C:\Documents and Settings\Administrator>ping 1.1.1.10

Pinging 1.1.1.10 with 32 bytes of data:

Reply from 1.1.1.10: bytes=32 time<1ms TTL=127
Reply from 1.1.1.10: bytes=32 time<1ms TTL=127
Reply from 1.1.1.10: bytes=32 time<1ms TTL=127
Reply from 1.1.1.10: bytes=32 time<1ms TTL=127

Ping statistics for 1.1.1.10:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\Documents and Settings\Administrator>_
```

图 6-190　验证测试

```
C:\Tools>nc -v -l -p 389
listening on [any] 389 ...
```

图 6-191　实施缓冲区溢出攻击(1)

```
C:\Documents and Settings\Administrator>netstat -an

Active Connections

  Proto  Local Address          Foreign Address        State
  TCP    0.0.0.0:21             0.0.0.0:0              LISTENING
  TCP    0.0.0.0:22             0.0.0.0:0              LISTENING
  TCP    0.0.0.0:80             0.0.0.0:0              LISTENING
  TCP    0.0.0.0:135            0.0.0.0:0              LISTENING
  TCP    0.0.0.0:389            0.0.0.0:0              LISTENING
  TCP    0.0.0.0:443            0.0.0.0:0              LISTENING
  TCP    0.0.0.0:445            0.0.0.0:0              LISTENING
  TCP    0.0.0.0:990            0.0.0.0:0              LISTENING
  TCP    0.0.0.0:3389           0.0.0.0:0              LISTENING
  TCP    127.0.0.1:1025         0.0.0.0:0              LISTENING
  TCP    127.0.0.1:43958        0.0.0.0:0              LISTENING
```

图 6-192　实施缓冲区溢出攻击(2)

在外部 PC(攻击主机)的命令行界面中运行 imap_exp. exe 进行攻击,命令格式如图 6-193 所示。

此时进入 USG 配置页面,即“本地日志”页面,选择“入侵防御日志”选项卡,可以看到 USG 检测到该缓冲区溢出攻击,并进行了告警,且动作为“丢弃会话”(DROP_SESSION),如图 6-194 所示。

### 7. 实施 IIS 服务攻击

在外部 PC(攻击主机)上运行 GUI_Unicode. exe 程序进行攻击,如图 6-195 所示。

此时进入 USG 配置页面,即“本地日志”页面,选择“入侵防御日志”选项卡,可以看到 USG 检测到该攻击,并进行告警,且动作为复位连接 RESET,如图 6-196 所示。

```
C:\WINDOWS\system32\cmd.exe

C:\>cd tools

C:\Tools>imap_exp

THCimail v0.1 - Imail LDAP exploit
tested on Imail 6-8
by Johnny Cyberpunk (jcyberpunk@thc.org)

Usage: <Host> <OS> <Imail Version>
Sample: THCimail 194.44.55.56 0 1

OS:
0 - Windows 2000 Server english all service packs
1 - Windows 2000 Professional german
2 - Windows XP SP1 german

Imail Version:
0 - Imail 6+7
1 - Imail 8

C:\Tools>imap_exp 1.1.1.10 0 1

THCimail v0.1 - Imail LDAP exploit
tested on Imail 6-8
by Johnny Cyberpunk (jcyberpunk@thc.org)
imailver = 68

[*] building buffer
[*] connecting the target
[*] Exploit send successfully ! Sleeping a while ....
[*] Trying to get a shell
```

图 6-193　外部攻击主机使用命令攻击




图 6-194　选择“入侵防御日志”选项卡

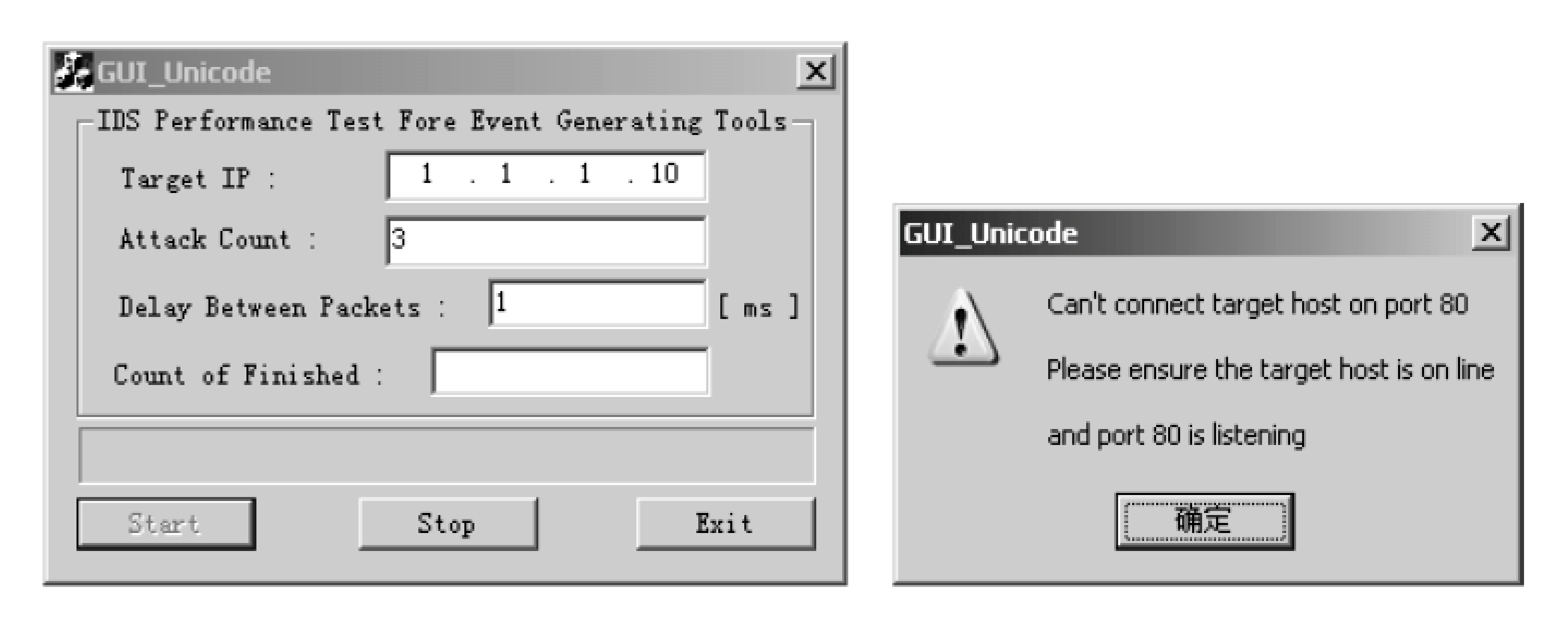



图 6-195　实施 IIS 服务攻击





| # | 名称 | 时间 | 类型 | 优先级 | 动作 | 防火墙ID |
|---|---|---|---|---|---|---|
| 1 | HTTP_MS_IIS_4.0/5.0_Unicode解码错误可远程执行命令漏洞利用 | 2008-09-02 18:18:13 | 安全漏洞 | 告警 | RESET | 1 |
| 2 | HTTP_MS_IIS_4.0/5.0_Unicode目录遍历尝试 | 2008-09-02 18:18:13 | CGI攻击 | 通知 | PASS | 1 |
| 3 | HTTP_目录遍历[../] | 2008-09-02 18:18:13 | CGI访问 | 通知 | PASS | 1 |
| 4 | TCP_Ipswitch_IMail_LDAP_Daemon_远程缓冲区溢出漏洞利用 | 2008-09-02 18:17:53 | 缓冲溢出 | 告警 | DROP_SESSION | 1 |

图 6-196　选择"入侵防御日志"选项卡

## 【注意事项】

本实验涉及的攻击工具只能用于实验。

# 6.10 会话监控与管理

## 【实验名称】

会话监控与管理。

## 【实验目的】

监控 USG(统一安全网关)中的会话流,并对会话进行管理。

## 【背景描述】

某公司使用 USG 作为网络出口设备连接到 Internet,并且公司内部有一台对外提供服务的服务器。最近网络管理员发现,在网络中出现大量来自 Internet 的访问服务器的连接,消耗了服务器大量系统资源。管理员怀疑该现象是恶意行为所导致,并希望能够及时将攻击源进行阻断。

## 【需求分析】

通过监控 USG 的会话表,可以查看流经 USG 的非法的、恶意的连接,并且对该会话进行阻断。

## 【实验拓扑】

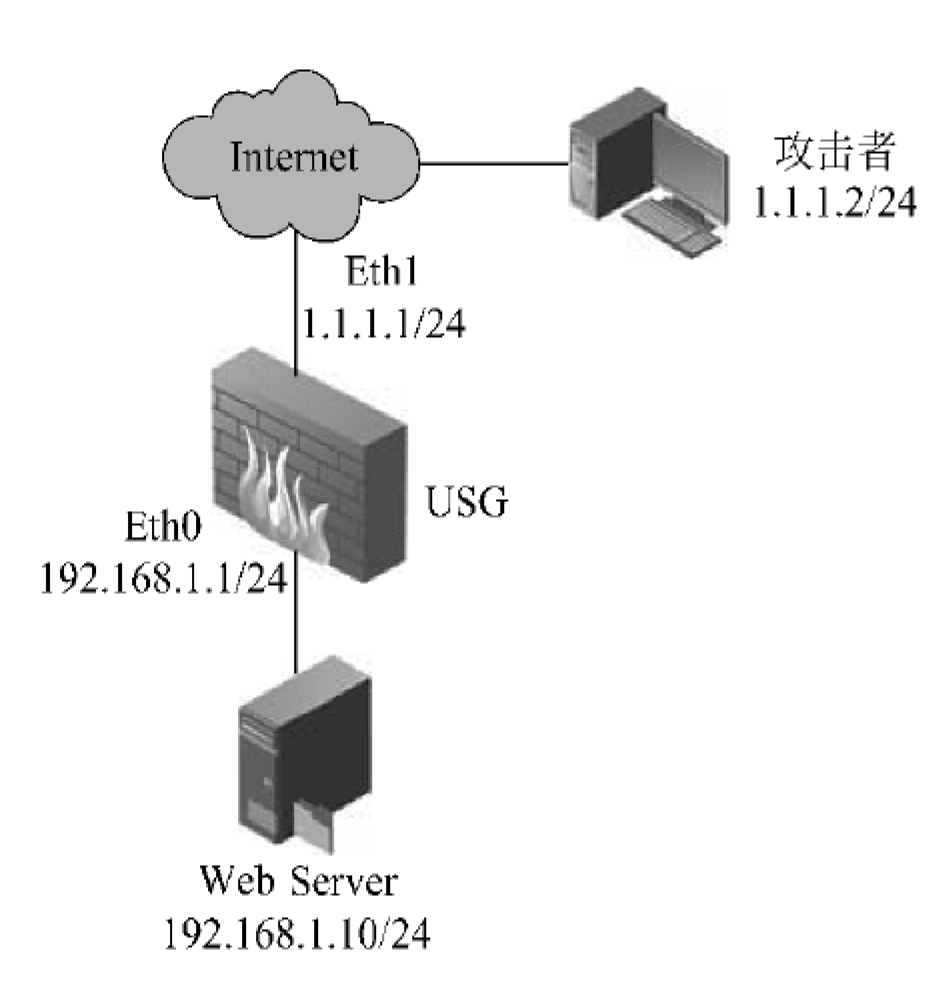




图 6-197　会话监控与管理网络拓扑图

如图 6-197 所示的网络拓扑,是企业为了提高网络的安全,购买了一台 RG-USG 统一安全网关,作为网络出口设备连接到 Internet,并且公司内部有一台对外提供服务的服务器。最近网络管理员发现,在网络中出现大量来自

Internet 的访问服务器的连接，消耗了服务器大量系统资源。管理员怀疑该现象是恶意行为所导致，并希望能够及时地将攻击源进行阻断。现在需要登录到 USG 并对其进行基本配置，通过监控 USG 的会话表，可以查看流经 USG 的非法的、恶意的连接，并且对该会话进行阻断，以实现网络的安全防范功能。

## 【实验设备】

USG　1 台
PC　　2 台（一台作为 Web 服务器；另一台模拟外部网络的攻击者）
TCP 连接工具

## 【预备知识】

- 网络基础知识。
- USG 操作基础知识。

## 【实验原理】

USG 提供了强大的监控功能，可以查看到通过 USG 的连接和会话，并且提供了对会话的管理限制功能，可以及时对可疑的会话进行阻断。

## 【实验步骤】

### 1. 配置 USG 接口的 IP 地址

如图 6-198 所示，进入 USG 的配置页面，即“接口”页面。

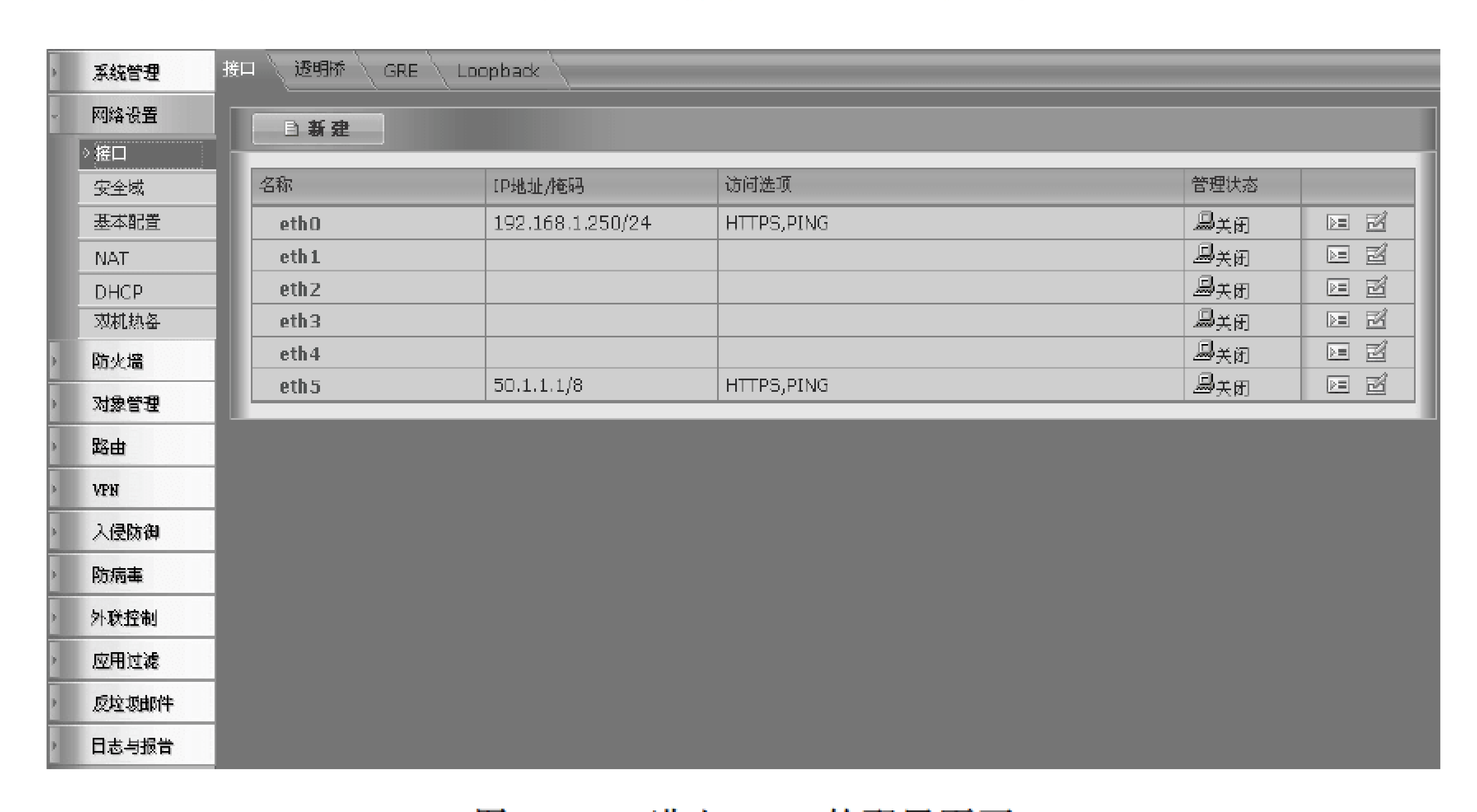



图 6-198　进入 USG 的配置页面

单击 eth0 接口的“编辑”图标，为 eth0 接口配置 IP 地址及子网掩码，如图 6-199 所示。

单击 eth1 接口的“编辑”图标，为 eth1 接口配置 IP 地址及子网掩码，如图 6-200 所示。

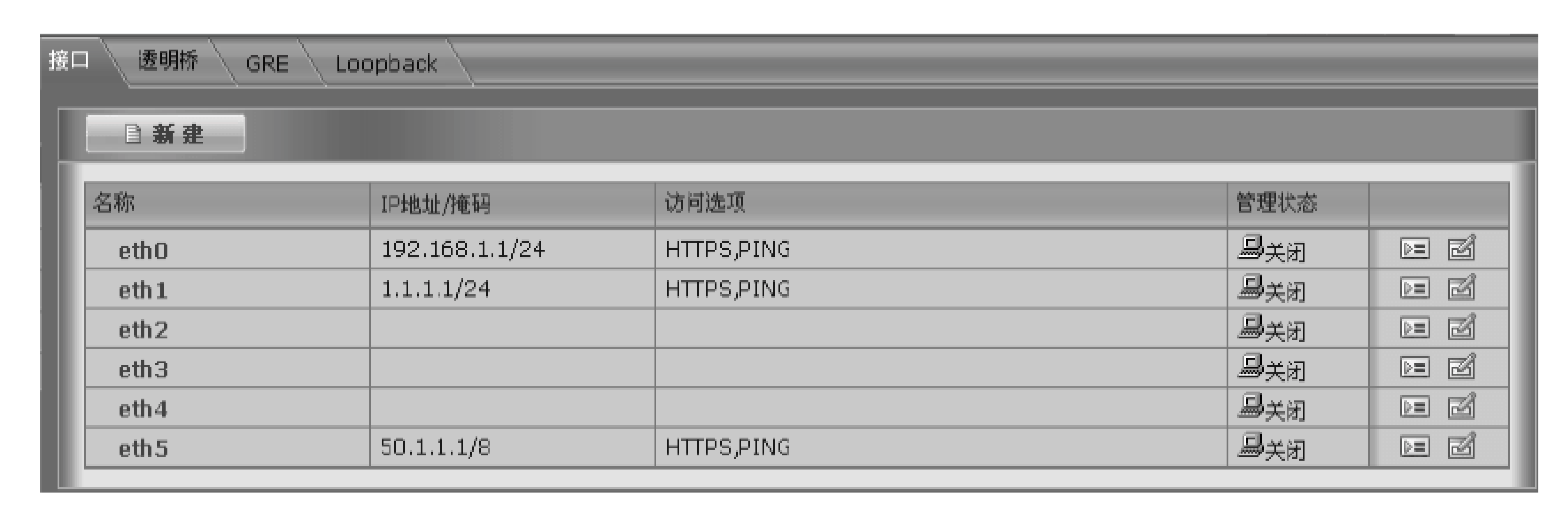



图 6-199 为 eth0 接口配置 IP 地址




图 6-200 为 eth1 接口配置 IP 地址

接口配置 IP 地址后的状态如图 6-201 所示。




| 名称 | IP地址/掩码 | 访问选项 | 管理状态 | |
|---|---|---|---|---|
| eth0 | 192.168.1.1/24 | HTTPS,PING | 关闭 | |
| eth1 | 1.1.1.1/24 | HTTPS,PING | 关闭 | |
| eth2 | | | 关闭 | |
| eth3 | | | 关闭 | |
| eth4 | | | 关闭 | |
| eth5 | 50.1.1.1/8 | HTTPS,PING | 关闭 | |

图 6-201 接口配置 IP 地址后的状态

## 2 配置静态 NAT 转换

为了使 Internet 中的用户可以访问内部的 Web 服务器，需要在 USG 上配置静态 NAT 转换，将 Web 服务器发布到 Internet 中，如图 6-202 所示。

进入USG配置页面，即NAT页面，选择“静态地址转换”单选按钮。




图6-202　配置静态NAT转换

单击“新建”按钮创建静态地址转换规则。规则中的“外部地址”为Web服务器对外发布的地址；“内部地址”为Web服务器实际的内部地址；“外部接口”为连接Internet的eth1接口，如图6-203所示。




图6-203　创建静态地址转换规则

## 3.配置安全策略

首先进入USG配置页面，即“地址对象”页面，配置包含内部FTP服务器的地址对象，如图6-204所示。

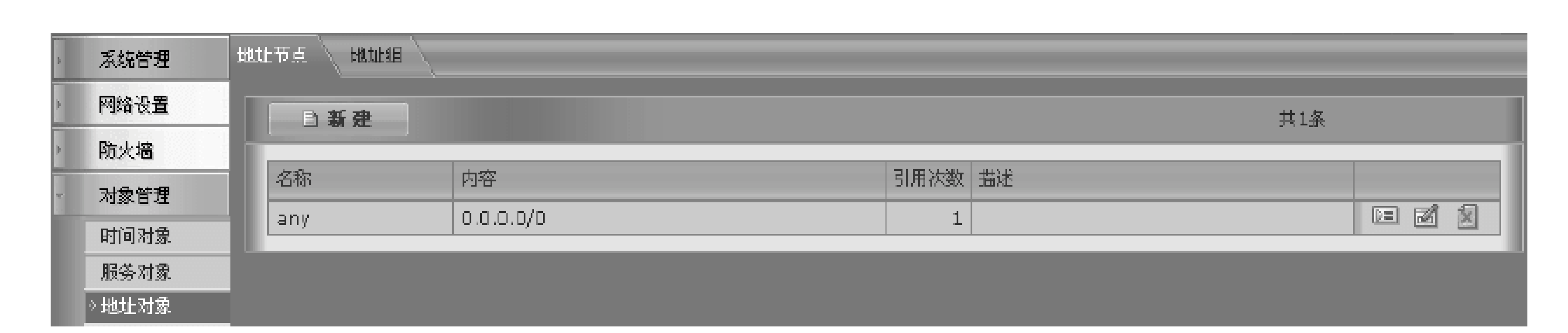



图6-204　配置安全策略

单击“新建”按钮创建地址对象，地址为Web服务器的内部地址192.168.1.10，如图6-205所示。

进入USG配置页面，即“安全策略”页面，配置允许外部访问FTP服务器的安全策略。

单击“新建”按钮创建安全策略。在安全策略中源接口为eth1接口；源地址为any地址对象；目的接口为eth0接口；目的地址为Server地址对象；服务为http服务对象；时间表为always地址对象，代表任何时间；动作为PERMIT允许，如图6-206所示。

创建完安全策略后，需要选择“启用”选项使该规则生效，如图6-207所示。

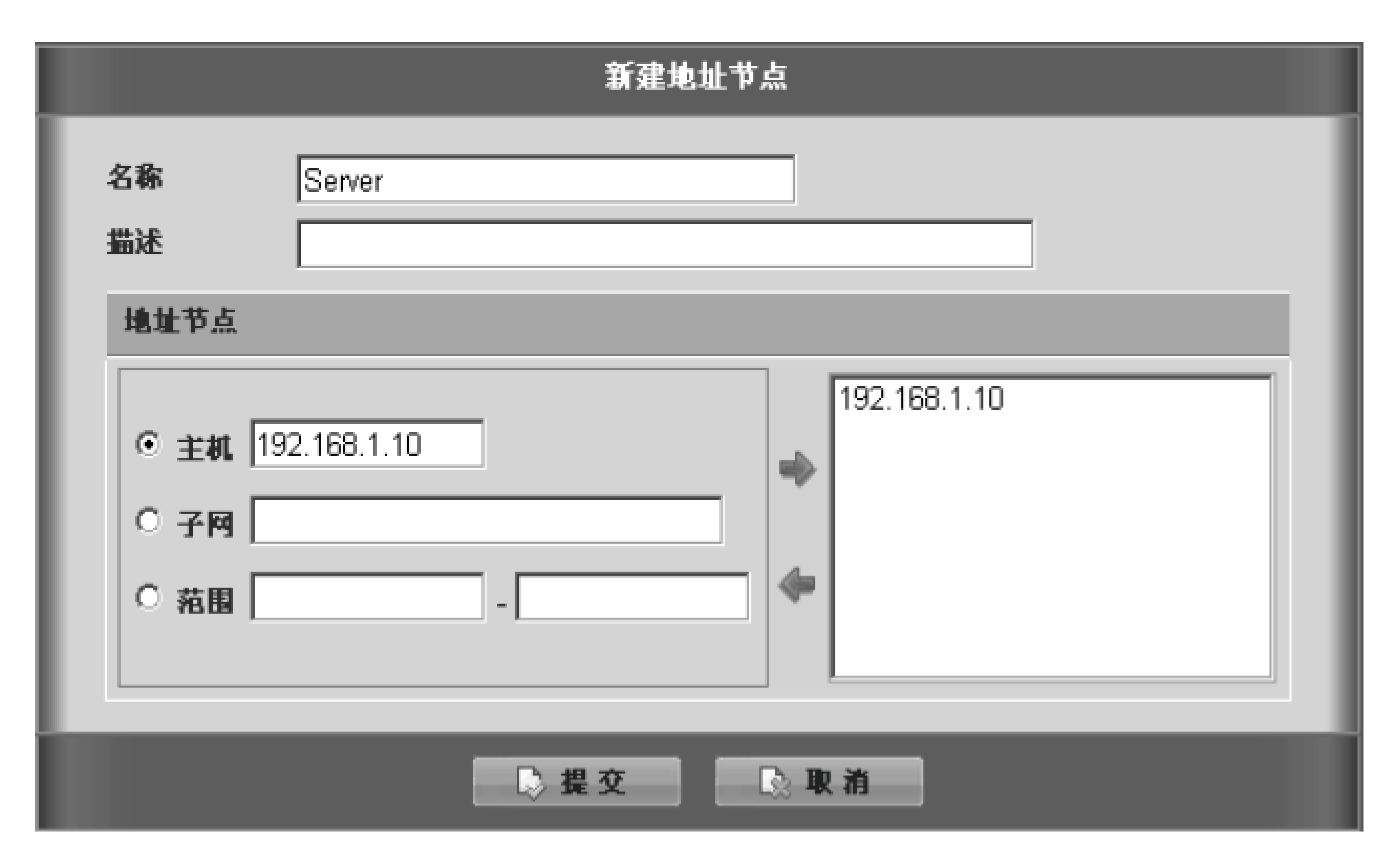



图 6-205　创建地址对象




图 6-206　配置 FTP 服务器安全策略




图 6-207　启用安全策略

### 4. 验证测试

在内部 PC 上搭建 Web 服务器,并进行相应的配置。在外部 PC 上测试访问 Web 服务器的连通性,注意这里使用的目标地址为 1.1.1.10。

### 5. 建立到达 Web 服务器的连接

在外部 PC 上使用 TCP 连接工具向 Web 服务器(1.1.1.10)建立大量的连接。此时在 Web 服务器上通过 Windows 命令 netstat -an 可以看到外部主机与 Web 服务器的 80

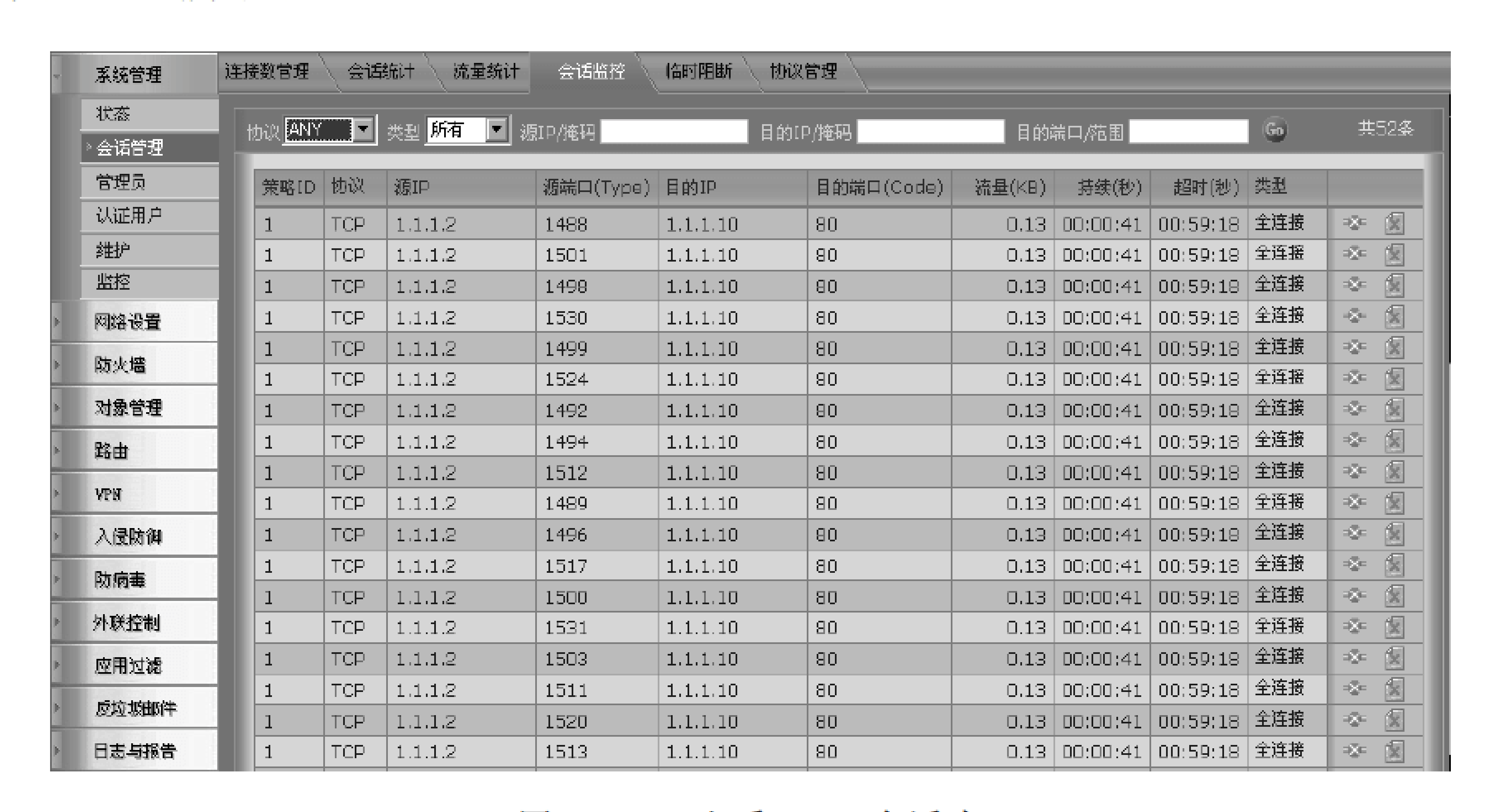
端口建立了大量的 TCP 连接，如图 6-208 所示。

```
C:\WINDOWS\system32\cmd.exe
  TCP    192.168.1.10:80        1.1.1.2:1338           ESTABLISHED
  TCP    192.168.1.10:80        1.1.1.2:1339           ESTABLISHED
  TCP    192.168.1.10:80        1.1.1.2:1340           ESTABLISHED
  TCP    192.168.1.10:80        1.1.1.2:1341           ESTABLISHED
  TCP    192.168.1.10:80        1.1.1.2:1342           ESTABLISHED
  TCP    192.168.1.10:80        1.1.1.2:1343           ESTABLISHED
  TCP    192.168.1.10:80        1.1.1.2:1344           ESTABLISHED
  TCP    192.168.1.10:80        1.1.1.2:1345           ESTABLISHED
  TCP    192.168.1.10:80        1.1.1.2:1346           ESTABLISHED
  TCP    192.168.1.10:80        1.1.1.2:1347           ESTABLISHED
  TCP    192.168.1.10:80        1.1.1.2:1348           ESTABLISHED
  TCP    192.168.1.10:80        1.1.1.2:1349           ESTABLISHED
  TCP    192.168.1.10:80        1.1.1.2:1350           ESTABLISHED
  TCP    192.168.1.10:80        1.1.1.2:1351           ESTABLISHED
  TCP    192.168.1.10:80        1.1.1.2:1352           ESTABLISHED
  TCP    192.168.1.10:80        1.1.1.2:1353           ESTABLISHED
  TCP    192.168.1.10:80        1.1.1.2:1354           ESTABLISHED
  TCP    192.168.1.10:80        1.1.1.2:1355           ESTABLISHED
  TCP    192.168.1.10:80        1.1.1.2:1356           ESTABLISHED
  TCP    192.168.1.10:80        1.1.1.2:1357           ESTABLISHED
  TCP    192.168.1.10:80        1.1.1.2:1358           ESTABLISHED
  TCP    192.168.1.10:80        1.1.1.2:1359           ESTABLISHED
  TCP    192.168.1.10:80        1.1.1.2:1360           ESTABLISHED
  TCP    192.168.1.10:80        1.1.1.2:1361           ESTABLISHED
  TCP    192.168.1.10:80        1.1.1.2:1362           ESTABLISHED
```

图 6-208　建立访问 Web 服务器连接

### 6. 查看 USG 会话表

进入 USG 配置页面，即“会话管理”页面，选择“会话监控”选项卡，单击Go按钮可以查看 USG 的会话状态表，可以看到大量来自 1.1.1.2 访问 1.1.1.10 的 80 端口的全连接，如图 6-209 所示。




| 策略ID | 协议 | 源IP | 源端口(Type) | 目的IP | 目的端口(Code) | 流量(KB) | 持续(秒) | 超时(秒) | 类型 |
|---|---|---|---|---|---|---|---|---|---|
| 1 | TCP | 1.1.1.2 | 1488 | 1.1.1.10 | 80 | 0.13 | 00:00:41 | 00:59:18 | 全连接 |
| 1 | TCP | 1.1.1.2 | 1501 | 1.1.1.10 | 80 | 0.13 | 00:00:41 | 00:59:18 | 全连接 |
| 1 | TCP | 1.1.1.2 | 1498 | 1.1.1.10 | 80 | 0.13 | 00:00:41 | 00:59:18 | 全连接 |
| 1 | TCP | 1.1.1.2 | 1530 | 1.1.1.10 | 80 | 0.13 | 00:00:41 | 00:59:18 | 全连接 |
| 1 | TCP | 1.1.1.2 | 1499 | 1.1.1.10 | 80 | 0.13 | 00:00:41 | 00:59:18 | 全连接 |
| 1 | TCP | 1.1.1.2 | 1524 | 1.1.1.10 | 80 | 0.13 | 00:00:41 | 00:59:18 | 全连接 |
| 1 | TCP | 1.1.1.2 | 1492 | 1.1.1.10 | 80 | 0.13 | 00:00:41 | 00:59:18 | 全连接 |
| 1 | TCP | 1.1.1.2 | 1494 | 1.1.1.10 | 80 | 0.13 | 00:00:41 | 00:59:18 | 全连接 |
| 1 | TCP | 1.1.1.2 | 1512 | 1.1.1.10 | 80 | 0.13 | 00:00:41 | 00:59:18 | 全连接 |
| 1 | TCP | 1.1.1.2 | 1489 | 1.1.1.10 | 80 | 0.13 | 00:00:41 | 00:59:18 | 全连接 |
| 1 | TCP | 1.1.1.2 | 1496 | 1.1.1.10 | 80 | 0.13 | 00:00:41 | 00:59:18 | 全连接 |
| 1 | TCP | 1.1.1.2 | 1517 | 1.1.1.10 | 80 | 0.13 | 00:00:41 | 00:59:18 | 全连接 |
| 1 | TCP | 1.1.1.2 | 1500 | 1.1.1.10 | 80 | 0.13 | 00:00:41 | 00:59:18 | 全连接 |
| 1 | TCP | 1.1.1.2 | 1531 | 1.1.1.10 | 80 | 0.13 | 00:00:41 | 00:59:18 | 全连接 |
| 1 | TCP | 1.1.1.2 | 1503 | 1.1.1.10 | 80 | 0.13 | 00:00:41 | 00:59:18 | 全连接 |
| 1 | TCP | 1.1.1.2 | 1511 | 1.1.1.10 | 80 | 0.13 | 00:00:41 | 00:59:18 | 全连接 |
| 1 | TCP | 1.1.1.2 | 1520 | 1.1.1.10 | 80 | 0.13 | 00:00:41 | 00:59:18 | 全连接 |
| 1 | TCP | 1.1.1.2 | 1513 | 1.1.1.10 | 80 | 0.13 | 00:00:41 | 00:59:18 | 全连接 |

图 6-209　查看 USG 会话表

### 7. 阻断会话

如果在会话表中发现可疑的会话，那么可以单击会话的阻断图标，这时我们可以建立临时阻断条目，这里认为来自 1.1.1.2 的会话为恶意连接，因此需要阻断其建立连接。可以单击会话的删除图标来清除该会话。

在建立阻断条目时，我们可以指定协议、源地址信息、目的地址信息、源端口号、目的端口号和阻断时间，并且在该时间内禁止符合阻断条目的会话通过。在本实验中我们阻断了 1.1.1.2 访问 Web 服务器的连接，如图 6-210 所示。




图 6-210　阻断会话

创建完临时阻断条目后，可以再配置页面，即“会话管理”页面，选择“临时阻断”选项卡，查看阻断条目，如图 6-211 所示。




图 6-211　查看阻断条目

## 8. 验证测试

在外部 PC 上再次使用 TCP 连接工具向 Web 服务器(1.1.1.10)建立大量的连接。此时在 Web 服务器上通过 Windows 命令 netstat-an 可以看到没有任何连接建立，因为 USG 已经将会话建立请求丢弃，如图 6-212 所示。

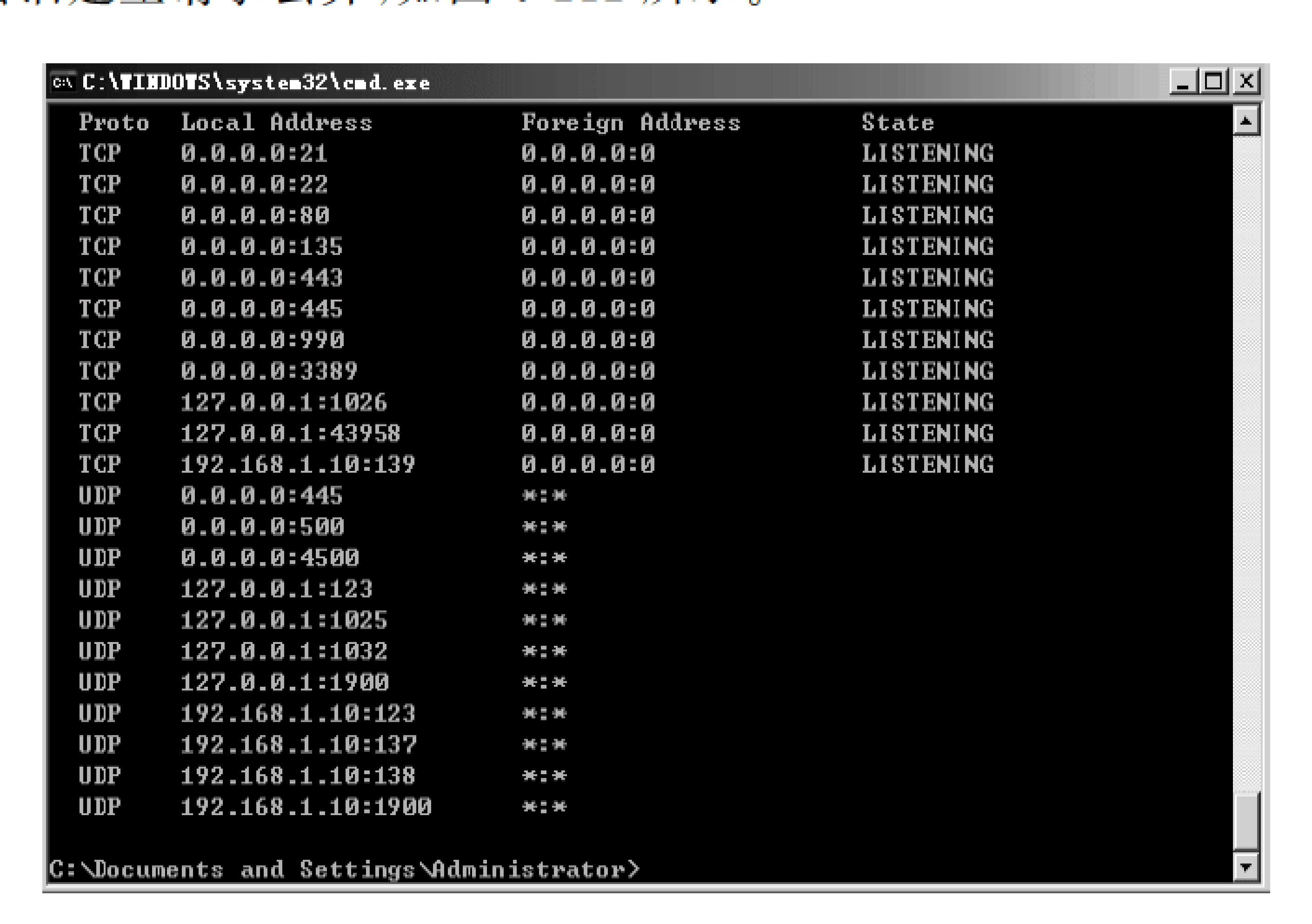



图 6-212　验证测试

## 【注意事项】

TCP 连接工具只能用于实验。






# 网络安全综合实验

# 第 7 章 构建安全的园区网络

## 【实验名称】

构建安全的园区网络。

## 【实验目的】

使用防火墙、安全 VPN、IDS 等技术构建安全的园区网络。

## 【背景描述】

某企业总部位于北京,并且在上海拥有办事处。总部通过一台防火墙接入 Internet,上海办事处通过一台 VPN 网关接入 Internet。公司总部和办事处网络都使用私有编址方案。总部网络内有一台提供对外服务的 FTP 服务器,这个服务器需要能被 Internet 上的用户访问到。

由于公司业务需要,总部和办事处之间需要共享业务信息,由于总部和办事处之间需要交互一些重要数据信息,所以这些信息在跨越不安全的 Internet 上进行传输时需要保证数据的机密性。此外,公司还经常有出差在外进行移动办公的人员,这些移动办公人员也都需要接入到总部网络以获取业务信息。

此外,为了提高网络的安全性,总部网络需要一种机制能够检测到网络中出现的安全威胁,以便及时地对威胁进行控制、阻断或隔离。

最后,总部网络希望运营商能够协助阻挡一些私有地址的 IP 欺骗攻击。

## 【需求分析】

需求 1:总部网络和办事处网络使用私有编址方案,但是需要访问 Internet 资源。

分析 1:使用私有编址方案接入到 Internet,在防火墙和 VPN 网关上采用安全 NAT。

需求 2:总部网络中的 FTP 需要对外提供服务。

分析 2:为了使内部 FTP 服务器能够对外提供服务,需要在总部防火墙上使用 IP 映射将 FTP 服务器发布到 Internet 中。

需求 3:总部和办事处网络需要共享信息,并且要保证数据传输的安全性。

分析 3:在总部网络和办事处网络之间构建安全的 IPSec 隧道,通过 IPSec 隧道传输的数据都将被进行加密处理。

需求 4:移动办公人员需要接入到总部网络获取信息。

分析 4：移动办公网络接入到 Internet 后，可以使用远程接入 IPSec 技术通过 IPSec 隧道接入到总部网络。

需求 5：总部网络内部需要能够检测安全威胁。

分析 5：在网络内部(防火墙后面)部署 IDS 可以对网络内部的数据进行监听和检测，并对检测到的威胁进行告警。

需求 6：Router 为运营商的路由器，要求其协助我们进行数据包过滤，防止源 IP 地址为私有地址的欺骗攻击到达总部网络。

分析 6：为了使运营商协助我们防止源 IP 地址为私有地址的欺骗攻击，需要在 Router 上使用 RFC 1918 过滤。

## 【实验拓扑】

如图 7-1 所示的网络拓扑，是某企业综合网络安全规划。由于业务需要，公司总部和办事处之间需要交互一些重要数据信息，所以这些信息在跨越不安全的 Internet 上进行传输时需要保证数据的机密性。公司还经常有出差在外进行移动办公的人员，这些移动办公人员也都需要接入到总部网络以获取业务信息，总部网络需要一种机制能够检测到网络中出现的安全威胁，以便及时对威胁进行控制、阻断或隔离，希望运营商能够协助阻挡一些私有地址的 IP 欺骗攻击。因此公司决定使用防火墙、安全 VPN、IDS 等技术构建全局安全的园区网络。

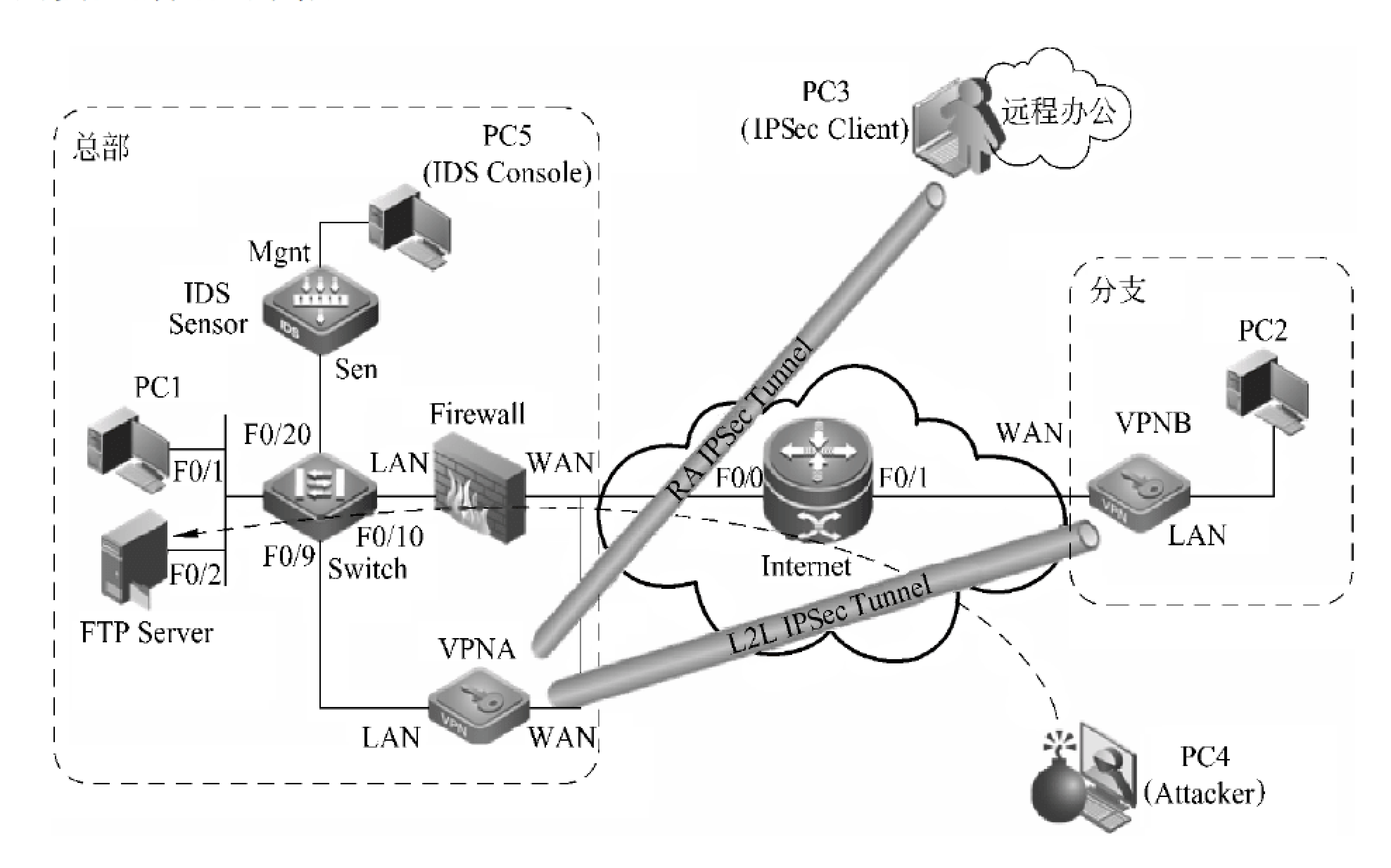



图 7-1　使用防火墙、安全 VPN、IDS 技术构建安全园区网络拓扑图

表 7-1 所示的地址信息，是企业使用防火墙、安全 VPN、IDS 技术构建如图 7-1 所示安全园区网络拓扑的地址规划情况。

表 7-1　地址信息

| 设备/接口 | IP 地 址 | 设备/接口 | IP 地 址 |
|---|---|---|---|
| PC1 | 192.168.1.3/24 | FW WAN | 200.1.1.1/24 |
| PC2 | 192.168.2.2/24 | VPNA LAN | 192.168.1.2/24 |
| PC3(IPSec Client) | 192.168.3.x/24(Private) | VPNA WAN | 200.1.1.3/24 |
| | 201.1.1.10/24(Public) | VPNB LAN | 192.168.2.1/24 |
| PC4(Attacker) | 201.1.1.44/24 | VPNB WAN | 201.1.1.1/24 |
| PC5(IDS Console) | 192.168.4.2/24 | Router F0/0 | 200.1.1.2/24 |
| FTP_Server | 192.168.1.100/24 | Router F0/1 | 201.1.1.2/24 |
| FW LAN | 192.168.1.1/24 | | |

## 【实验设备】

- 防火墙　1 台
- VPN 网关　2 台
- IDS　1 台
- 交换机　3 台
- PC　7 台(其中 PC1 和 PC2 用做子网用户,PC3 用做远程 IPSec 接入客户端,PC4 用做 Internet 攻击者,PC5 用做 IDS 控制台,一台 PC 用做 FTP Server,最后一台 PC 用做对于各个设备的管理机)
- 防火墙管理员证书
- 安全远程接入系统 SRA 安装程序
- 锐捷网关管理中心安装程序
- IDS 事件收集器安装程序
- IDS 控制台安装程序
- 端口扫描软件
- FTP Server 软件

## 【预备知识】

防火墙工作原理及基本配置、VPN 工作原理及基本配置、IDS 工作原理及基本配置、交换机基本配置、端口镜像原理。

## 【实验原理】

通过使用防火墙的安全 NAT 和访问控制功能,可以实现私有网络安全地接入到 Internet,并且将内部服务器发布到 Internet 中,使得 Internet 用户可以访问网络内部资源。利用 IPSec VPN 的安全功能可以使两个局域网通过在 Internet 上构建的安全加密隧道安全地进行数据传输,并且通过 IPSec 的远程接入可以使移动办公的用户接入到内

部网络共享资源。IDS 作为一个安全威胁检测系统,可以针对网络中的数据流进行监听和分析,当发现网络流量中存在安全威胁时,可以立即产生告警,后续可以使用相应的方法阻断或隔离威胁。对于报文的过滤,我们可以使用路由器的访问控制列表(ACL)来实现。

## 【实验流程图】

如图 7-2 所示的实验流程图,是企业使用防火墙、安全 VPN、IDS 技术,构建如图 7-1 所示安全园区的施工流程规划。在复杂项目施工前,通过规划施工过程流程,可以减少项目施工过程中的故障发生率,从而有效提高项目施工效率。

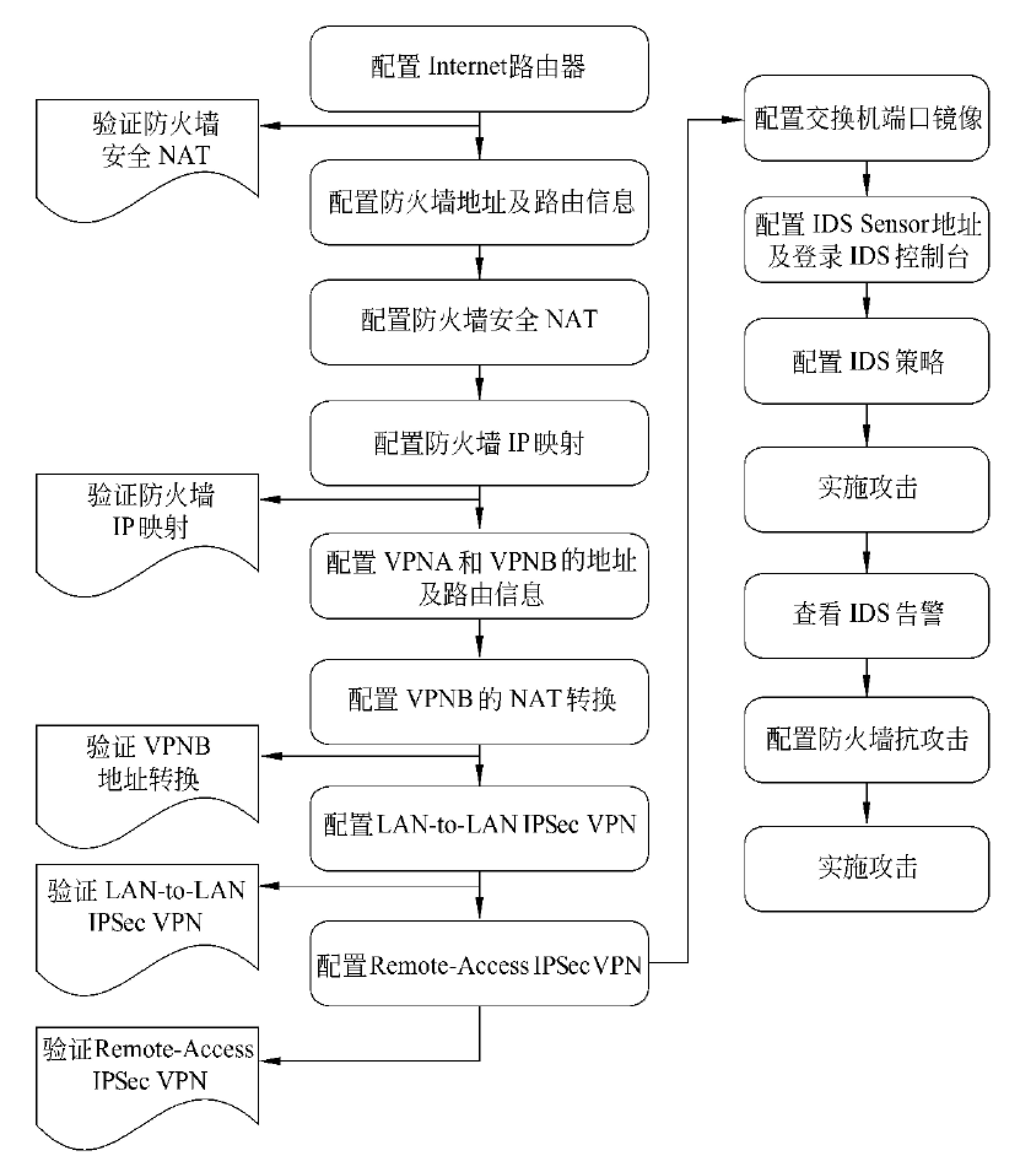



图 7-2　实验流程图

## 【实验步骤】

### 1. 配置 Internet 路由器以模拟 Internet 环境

```
Router# configure terminal
Router(config)# interface fastEthernet 0/0
Router(config-if)# ip address 200.1.1.2 255.255.255.0
```

```
Router(config-if)# exit
Router(config)# interface fastEthernet 0/1
Router(config-if)# ip address 201.1.1.2 255.255.255.0
Router(config-if)# exit
Router(config)#
```

**注意**：不要在路由器上配置访问总部网络和分支办事处网络私有子网的路由，因为 Internet 中的路由器是没有访问私有地址的路由条目的。

## 2 配置防火墙接口地址

在防火墙的Web界面中，选择“网络配置”→“接口IP”后进入地址配置页面，单击“添加”按钮为接口添加IP地址，如图7-3和图7-4所示。




图 7-3　配置防火墙接口地址(1)




图 7-4　配置防火墙接口地址(2)

为 LAN 接口和 WAN 接口添加完地址后的地址信息如图 7-5 所示。

| 网络接口 | 接口IP | 掩码 | 允许所有主机PING | 用于管理 | 允许管理主机PING | 允许管理主机Traceroute | 操作 |
|---|---|---|---|---|---|---|---|
| ADSL | 未启用 | | | | | | |
| DHCP | 未启用 | | | | | | |
| lan | 192.168.1.1 | 255.255.255.0 | ✔ | ✔ | ✔ | ✔ | |
| wan | 200.1.1.1 | 255.255.255.0 | ✖ | ✖ | ✖ | ✖ | |
| wan1 | 172.16.1.1 | 255.255.255.0 | ✔ | ✔ | ✔ | ✔ | |

添加 刷新

图 7-5　防火墙接口地址信息

### 3. 配置防火墙默认路由

在防火墙的 Web 界面中，选择“网络配置”→“策略路由”后进入路由配置页面，然后单击“添加”按钮添加一条默认路由，下一跳为 Internet 路由器 F0/0 接口的地址 200.1.1.2，如图 7-6 所示。




图 7-6　配置防火墙默认路由

单击“确定”按钮完成默认路由的添加，如图 7-7 所示。



| 类型 | 源地址 | 目的地址 | 下一跳 | 操作 |
|---|---|---|---|---|
| 路由 | any | 0.0.0.0/0.0.0.0 | 200.1.1.2 | |
| * | any | 200.1.1.0/255.255.255.0 | * | |
| * | any | 192.168.1.0/255.255.255.0 | * | |
| * | any | 172.16.1.0/255.255.255.0 | * | |

添加

图 7-7　添加防火墙默认路由

### 4. 配置防火墙安全 NAT

在防火墙的 Web 界面中，选择“安全策略”→“安全规则”后进入安全规则配置页面，然后单击页面上的“NAT 规则”按钮配置安全 NAT 规则。

在 NAT 规则中，源地址为被转换的地址 192.168.1.0/24，目的地址为 any，服务为 any，转换后的地址为 wan 接口的地址 200.1.1.1，数据的入接口为 lan 接口，出接口为 wan 接口，如图 7-8 所示。

配置完 NAT 规则后单击“确定”按钮完成规则的添加，添加后的规则如图 7-9 所示。




图 7-8　配置防火墙安全 NAT




图 7-9　添加防火墙安全 NAT 规则

### 5. 验证防火墙安全 NAT

将 PC1 的 IP 地址配置为 192.168.1.3/24，默认网关为防火墙 LAN 接口的地址 192.168.1.1。然后在 PC1 上 ping 路由器 F0/0 接口的地址 200.1.1.2，如图 7-10 所示。

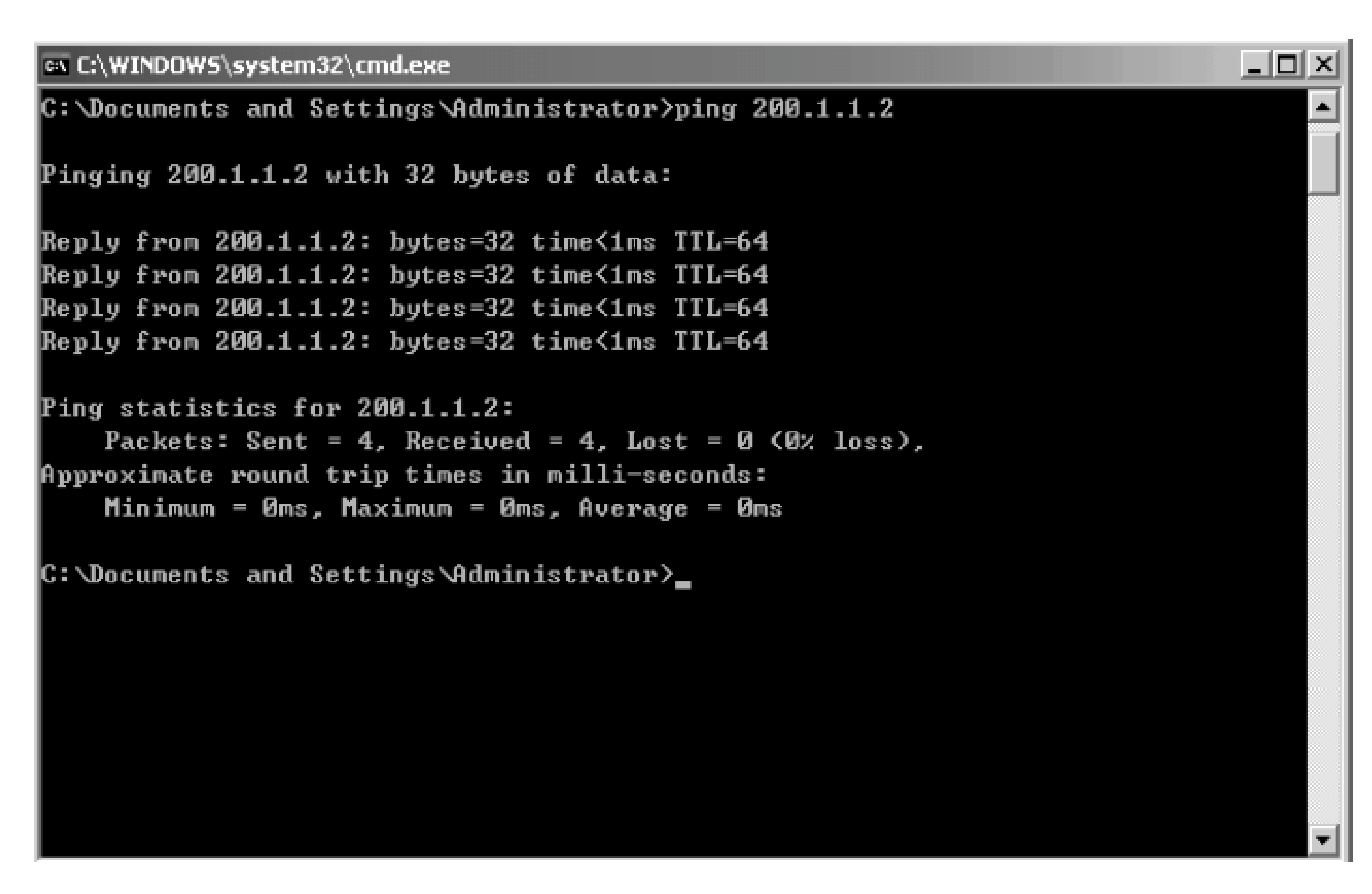



图 7-10　验证防火墙安全 NAT

通过 ping 的结果可以看到，PC1 通过防火墙的安全 NAT 可以访问 Internet（注意：由于 Internet 路由器上没有访问总部私有网络 192.168.1.0/24 的路由，所以如果 NAT 不生效，PC1 则无法访问 Internet）。

## 6. 配置防火墙 IP映射规则

使用与之前同样的方式为防火墙的 WAN 接口再添加一个 IP 地址 200.1.1.100/24，此地址用于发布内部 FTP 服务器。

在防火墙的 Web 界面中，选择“安全策略”→“安全规则”后进入安全规则配置页面，然后单击页面上的“IP 映射规则”按钮配置 IP 映射规则。IP 映射规则中的公开地址为 200.1.1.100，内部地址为 FTP 服务器的地址 192.168.1.100，入接口为 wan 接口，出接口为 lan 接口。这样当 Internet 用户访问 200.1.1.100 时，防火墙将把请求映射到内部的 FTP 服务器，如图 7-11 所示。




图 7-11 配置防火墙 IP 映射规则

配置完 IP 映射规则后，单击“确定”按钮完成规则的添加，如图 7-12 所示。



安全策略>>安全规则　　跳转到 全部

| 序号 | 规则名 | 源地址 | 目的地址 | 服务 | 类型 | 选项 | 生效 |
|---|---|---|---|---|---|---|---|
| 1 | nat1 | 192.168.1.0 | any | any | NAT规则 | | ✔ |
| 2 | ftpserver | 0.0.0.0 | 200.1.1.100 | any | IP映射 | | ✔ |

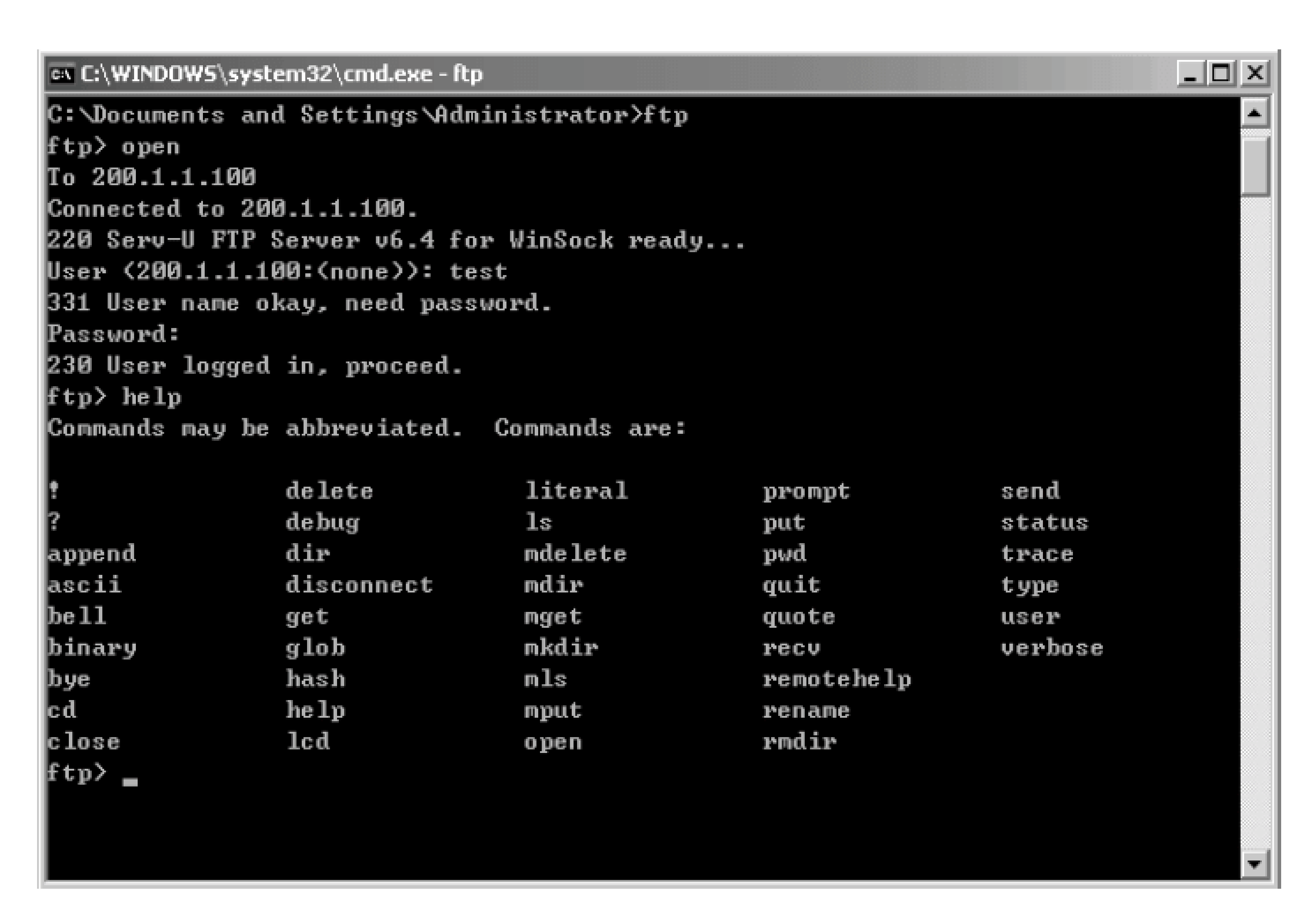
首页 上一页 下一页 尾页 第1页/1页 跳转到 1 页 确定 每页 100 行

图 7-12 添加防火墙 IP 映射规则

## 7. 验证防火墙 IP映射规则

将 PC3 的 IP 地址配置为 201.1.1.10/24，默认网关为 Internet 路由器 F0/1 接口的地址 201.1.1.2。

在总部网络上将 FTP 服务器的地址配置为 192.168.1.100/24，默认网关为 192.168.1.1。启动 FTP Server(需要预先安装 FTP Server 程序)，然后在 PC3 上对 FTP 服务器进行访问，访问 FTP 服务器使用地址 200.1.1.100。登录 FTP 服务器使用预先创建的用户名 test，密码为 test，如图 7-13 所示。


```
C:\Documents and Settings\Administrator>ftp
ftp> open
To 200.1.1.100
Connected to 200.1.1.100.
220 Serv-U FTP Server v6.4 for WinSock ready...
User (200.1.1.100:(none)): test
331 User name okay, need password.
Password:
230 User logged in, proceed.
ftp> help
Commands may be abbreviated.  Commands are:

!               delete          literal         prompt          send
?               debug           ls              put             status
append          dir             mdelete         pwd             trace
ascii           disconnect      mdir            quit            type
bell            get             mget            quote           user
binary          glob            mkdir           recv            verbose
bye             hash            mls             remotehelp
cd              help            mput            rename
close           lcd             open            rmdir
ftp>
```

图 7-13　验证防火墙 IP 映射规则

从图 7-13 可以看出，PC3 成功地通过地址 200.1.1.100 登录到 FTP 服务器上。由于在防火墙上配置了 200.1.1.100 至 192.168.1.3 的映射，所以防火墙会把 FTP 请求定向到内部的 FTP 服务器 192.168.1.3 上。

## 8. 配置 VPN 网关接口地址

连接到 VPN 网关的串口，使用命令行配置 VPNA 的接口地址：

```
Ruijie Co., Ltd.
Model: RG-WALL-V50
Version: RG-WALL-v2.30.10
http://www.ruijie.com.cn
mailto:service@star-net.cn
RG-WALL login: sadm                                    !默认用户名为 sadm
Password:                                              !默认密码为 sadm
[sadm@RG-WALL]# network
[sadm@RG-WALL(Network)]# interface set
Interface to set (eth0, eth1, Enter means cancel):
eth1                                                   !配置 VPNA WAN 接口的地址
Bring up onboot? (0: No, 1: Yes, Enter means Yes)
1
Work mode (0: UnCfg, 1: Manual, 2: DHCP, 3: PPPoE, 4: InBridge, Enter means Manual):
1
IP Address (xxx.xxx.xxx.xxx):
200.1.1.3
```

```
Netmask (xxx.xxx.xxx.xxx, Enter means 255.255.255.0):
255.255.255.0
GateWay (xxx.xxx.xxx.xxx, Enter means no default gateway in this network):
200.1.1.2                                !WAN接口的默认网关为 Internet路由器 F0/0接口地址
MAC Address (xx:xx:xx:xx:xx:xx, Enter means use MAC Address of device):

MTU (68-1500, Enter means use MTU of device):

Link-Guarantee Weight (1-255, Enter means 100):

[sadm@RG-WALL(Network)]# interface set
Interface to set (eth0, eth1, Enter means cancel):
eth0                                                      !配置 VPNA LAN接口的地址
Bring up onboot? (0: No, 1: Yes, Enter means Yes)
1
Work mode (0: UnCfg, 1: Manual, 2: DHCP, 3: PPPoE, 4: InBridge, Enter means Manual):
1
IP Address (xxx.xxx.xxx.xxx):
192.168.1.2
Netmask (xxx.xxx.xxx.xxx, Enter means 255.255.255.0):
255.255.255.0
GateWay (xxx.xxx.xxx.xxx, Enter means no default gateway in this network):
                                                          !在 LAN接口不配置默认网关
MAC Address (xx:xx:xx:xx:xx:xx, Enter means use MAC Address of device):

MTU (68-1500, Enter means use MTU of device):

[sadm@RG-WALL(Network)]# exit
[sadm@RG-WALL]# exit
```

连接到 VPN 网关的串口，使用命令行配置 VPNB 的接口地址：

```
Ruijie Co., Ltd.
Model: RG-WALL-V50
Version: RG-WALL-v2.30.10
http://www.ruijie.com.cn
mailto:service@star-net.cn
RG-WALL login: sadm                                 !默认用户名为 sadm
Password:                                           !默认密码为 sadm
[sadm@RG-WALL]# network
[sadm@RG-WALL(Network)]# interface set
Interface to set (eth0, eth1, Enter means cancel):
eth1                                                !配置 VPNB WAN接口的地址
Bring up onboot? (0: No, 1: Yes, Enter means Yes)
1
```

```
Work mode (0: UnCfg, 1: Manual, 2: DHCP, 3: PPPoE, 4: InBridge, Enter means Manual):
1
IP Address (xxx.xxx.xxx.xxx):
201.1.1.1
Netmask (xxx.xxx.xxx.xxx, Enter means 255.255.255.0):
255.255.255.0
GateWay (xxx.xxx.xxx.xxx, Enter means no default gateway in this network):
201.1.1.2                                  !WAN接口的默认网关为 Internet路由器 F0/1接口地址
MAC Address (xx:xx:xx:xx:xx:xx, Enter means use MAC Address of device):

MTU (68-1500, Enter means use MTU of device):

Link-Guarantee Weight (1-255, Enter means 100):

[sadm@RG-WALL(Network)]#interface set
Interface to set (eth0, eth1, Enter means cancel):
eth0                                                     !配置 VPNB LAN接口的地址
Bring up onboot? (0: No, 1: Yes, Enter means Yes)
1
Work mode (0: UnCfg, 1: Manual, 2: DHCP, 3: PPPoE, 4: InBridge, Enter means Manual):
1
IP Address (xxx.xxx.xxx.xxx):
192.168.2.1
Netmask (xxx.xxx.xxx.xxx, Enter means 255.255.255.0):
255.255.255.0
GateWay (xxx.xxx.xxx.xxx, Enter means no default gateway in this network):
                                                         !在 LAN接口不配置默认网关
MAC Address (xx:xx:xx:xx:xx:xx, Enter means use MAC Address of device):

MTU (68-1500, Enter means use MTU of device):

[sadm@RG-WALL(Network)]#exit
[sadm@RG-WALL]#exit
```

## 9. 配置 VPNB 的地址对象

通过 VPN 网关管理中心连接到 VPNB 的管理界面，选择“防火墙”→“对象管理”→“IP 地址对象”后进入 IP 地址对象配置页面，然后单击页面上的“添加对象”按钮创建一个新的 IP 地址对象，名称为“分支办事处”，单击“确定”按钮完成 IP 地址对象的添加，如图 7-14 所示。

IP 地址对象添加完毕后，选中“分支办事处”IP 地址对象，单击页面上的“添加成员”按钮，为该对象添加分支网络的子网地址 192.168.2.0/24，单击“确定”按钮完成地址配置，如图 7-15 所示。




图 7-14 配置 VPNB 的地址对象




图 7-15 为对象添加分支网络子网地址

## 10. 配置 VPNB 的 NAT 转换

在 VPNB 的管理界面中，选择“防火墙”→“访问规则”后进入访问规则配置页面，然后双击页面上序号为 1 的默认所有访问通过的规则，对其进行修改。

在访问规则配置框中，选择名为“分支办事处”的源对象，并在源转换的地址转换类型中选择“按转发接口自动转换”，并勾选“端口转换”复选框，这样 VPN 网关将对来自分支办事处子网的访问进行源地址端口转换，单击“确定”按钮完成修改，如图 7-16 所示。

修改完成的规则如图 7-17 所示。

## 11. 验证 VPNB 的地址转换

将 PC2 的 IP 地址配置为 192.168.2.2/24，默认网关为 VPNB 的 LAN 接口的地址 192.168.2.1，在 PC2 上 ping Internet 路由器 F0/1 接口的地址 201.1.1.2/24，如图 7-18 所示。

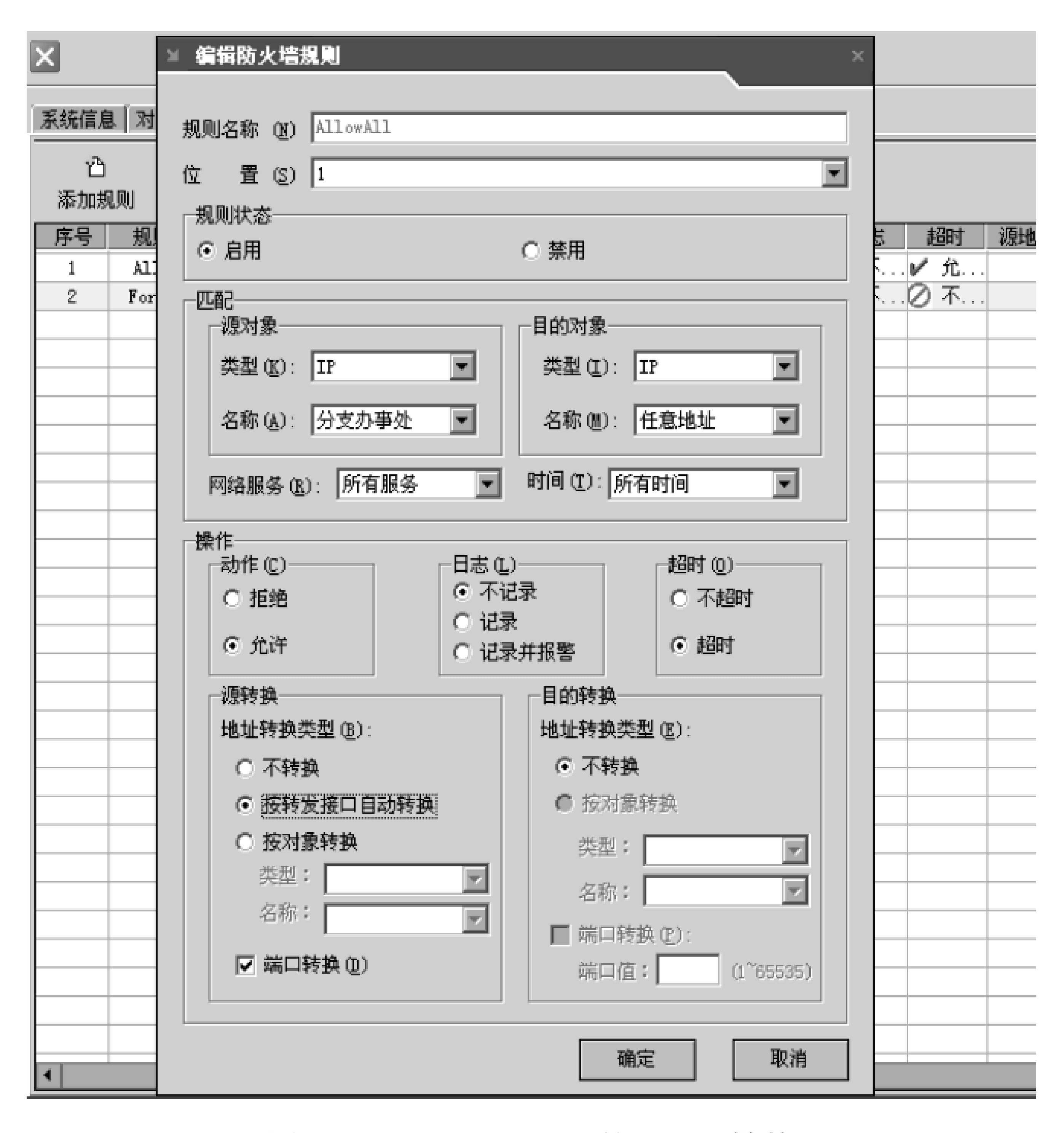
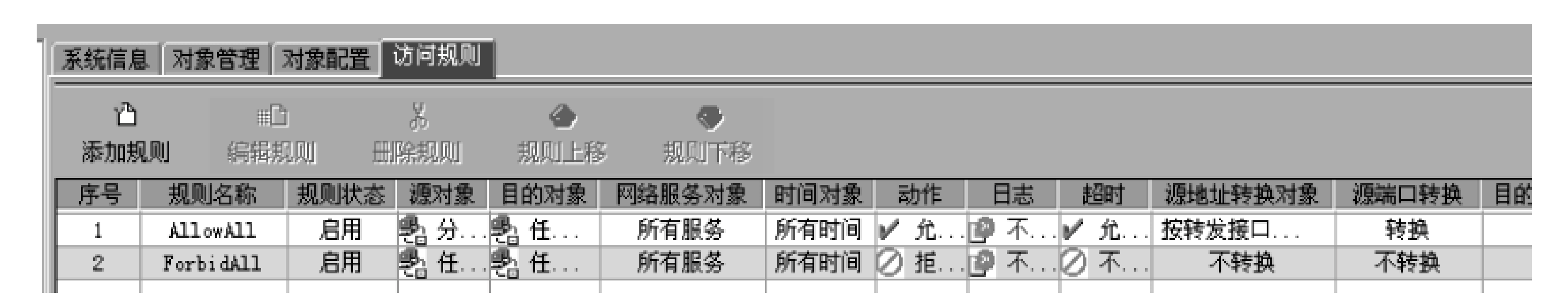
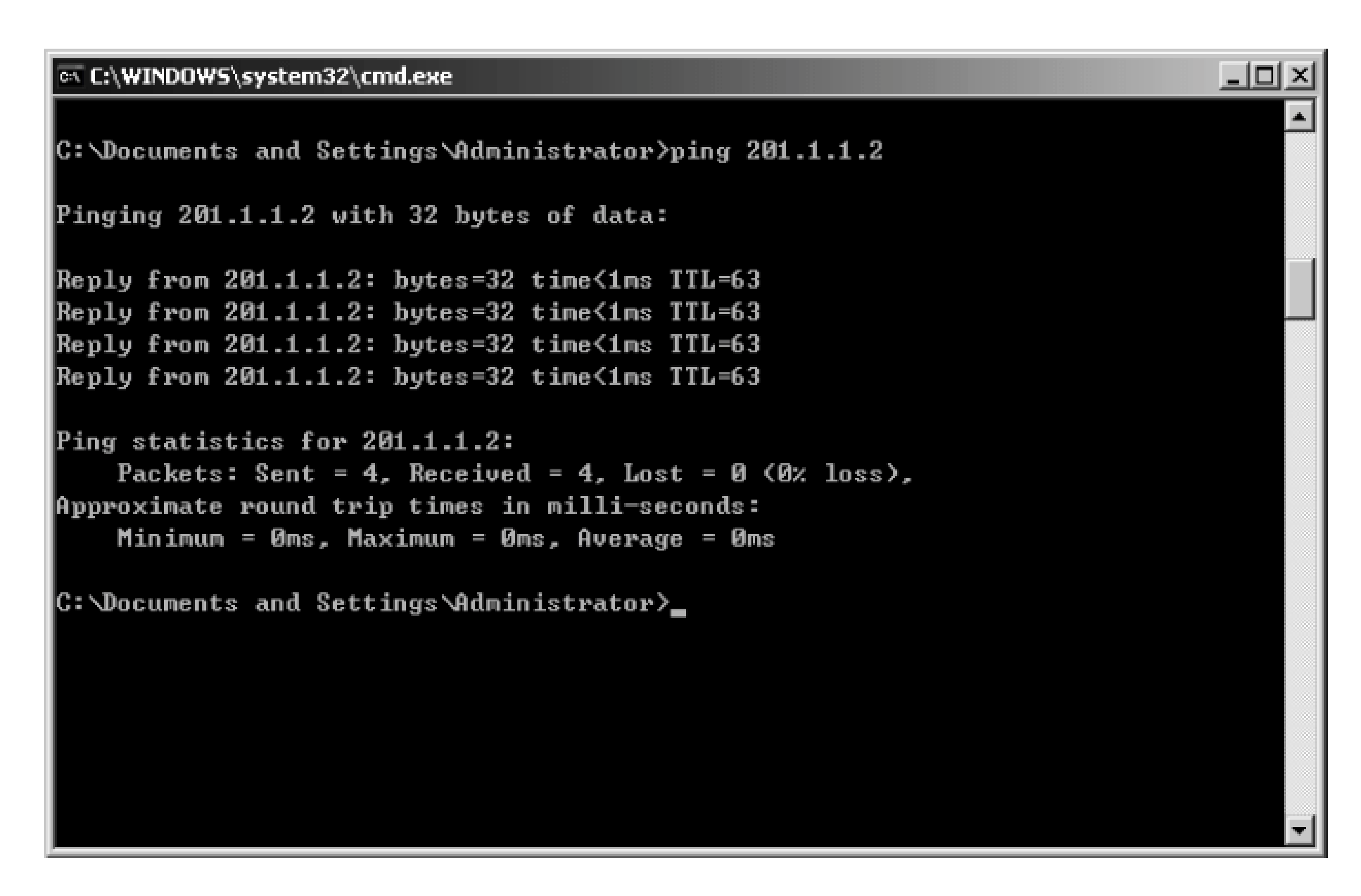


图 7-16　配置 VPNB 的 NAT 转换



| 序号 | 规则名称 | 规则状态 | 源对象 | 目的对象 | 网络服务对象 | 时间对象 | 动作 | 日志 | 超时 | 源地址转换对象 | 源端口转换 | 目的 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 1 | AllowAll | 启用 | 分… | 任… | 所有服务 | 所有时间 | 允… | 不… | 允… | 按转发接口… | 转换 | |
| 2 | ForbidAll | 启用 | 任… | 任… | 所有服务 | 所有时间 | 拒… | 不… | 不… | 不转换 | 不转换 | |

图 7-17　修改完成的规则



```
C:\Documents and Settings\Administrator>ping 201.1.1.2

Pinging 201.1.1.2 with 32 bytes of data:

Reply from 201.1.1.2: bytes=32 time<1ms TTL=63
Reply from 201.1.1.2: bytes=32 time<1ms TTL=63
Reply from 201.1.1.2: bytes=32 time<1ms TTL=63
Reply from 201.1.1.2: bytes=32 time<1ms TTL=63

Ping statistics for 201.1.1.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\Documents and Settings\Administrator>_
```

图 7-18　验证 VPNB 的地址转换

通过 ping 结果可以看出,VPNB 的 NAT 转换成功。

## 12. 配置 VPNA 的 LAN-to-LAN IPSec VPN

在 VPNA 的管理界面中,选择"虚拟专用网"→IPSec VPN→"隧道配置"后进入隧道配置页面,然后单击页面上的"添加设备"按钮配置对端 VPN 网关。

在"对方设备名称"文本框中输入对方 VPN 网关的名称,这里我们输入 VPNB;在"本地设备接口"下拉列表中选择在哪个接口上建立 IPSec 隧道,这里我们选择 WAN 接口 eht1;在"本地设备身份"区域中我们选择"作为客户端"单选按钮,并配置"对方设备地址"为 VPNB WAN 接口的地址 201.1.1.1;在"认证方式"区域中我们选择"预共享密钥"单选按钮,并将"密钥"设置为 1234567,单击"确定"按钮完成配置,如图 7-19 所示。




图 7-19 配置虚拟专用网

完成对端设备的配置后,单击页面上的"添加隧道"按钮配置访问 VPNB 的 IPSec 隧道。

在"隧道信息"选项卡中,"隧道名称"使我们可以为该隧道指定任意的名称,这里我们使用 To_VPNB;在"对方设备名称"下拉列表中选择刚刚创建的对端设备 VPNB;在"本地子网"区域中输入总部网络的子网信息 192.168.1.0/24;在"对方子网"区域中输入分支办事处网络的子网信息 192.168.2.0/24,如图 7-20 所示。

在"通信策略"选项卡中,对于 VPNB 的设备连接默认使用 IPSec 隧道模式。IPSec 默认使用 ESP 协议,加密算法为 3DES,哈希函数使用 SHA。这里也可以指定多个套件,双方会在多个中协商出一个匹配的套件来建立隧道,单击"确定"按钮完成隧道的配置,如图 7-21 所示。

完成后的隧道配置如图 7-22 所示。

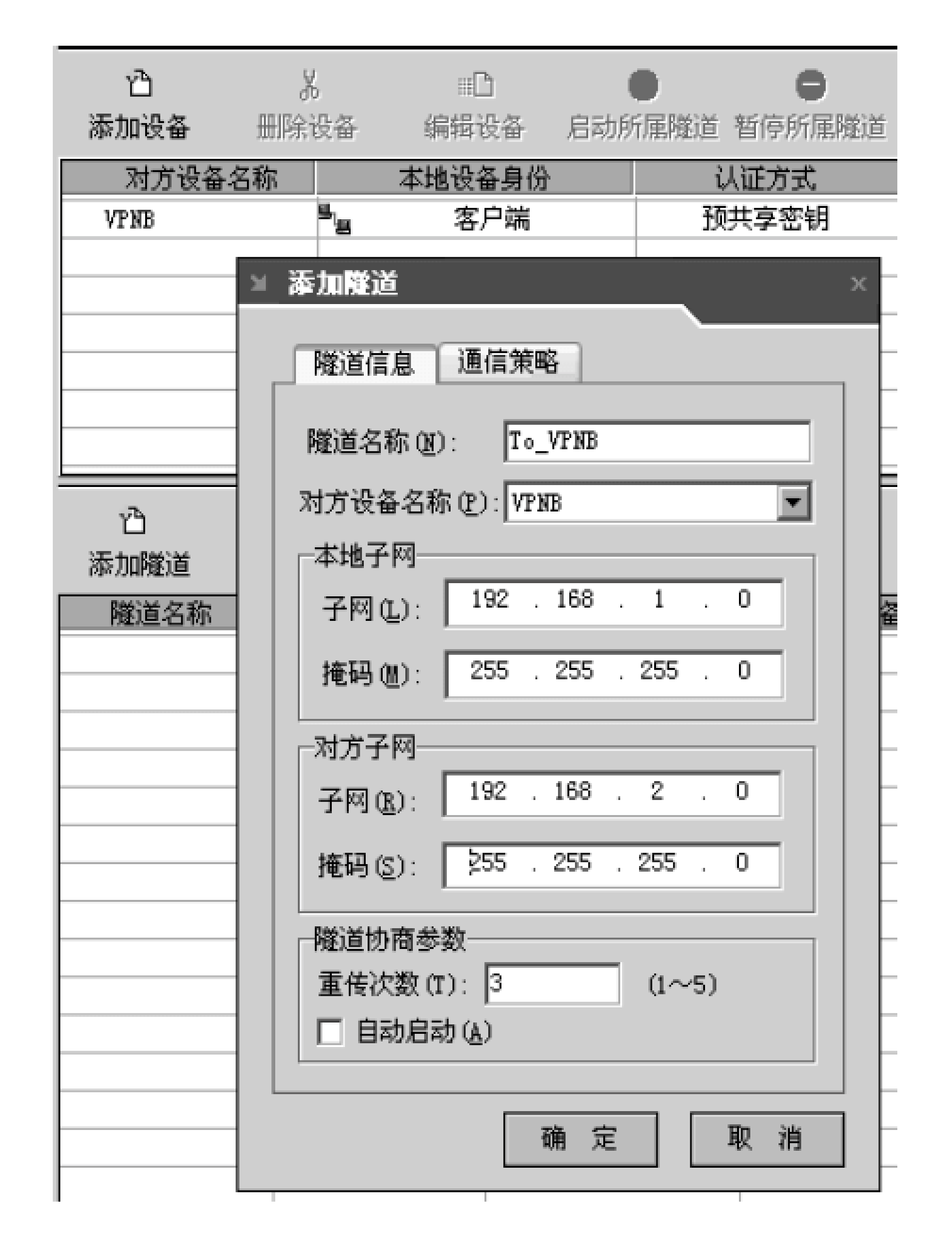



图 7-20　输入总部网络的子网信息

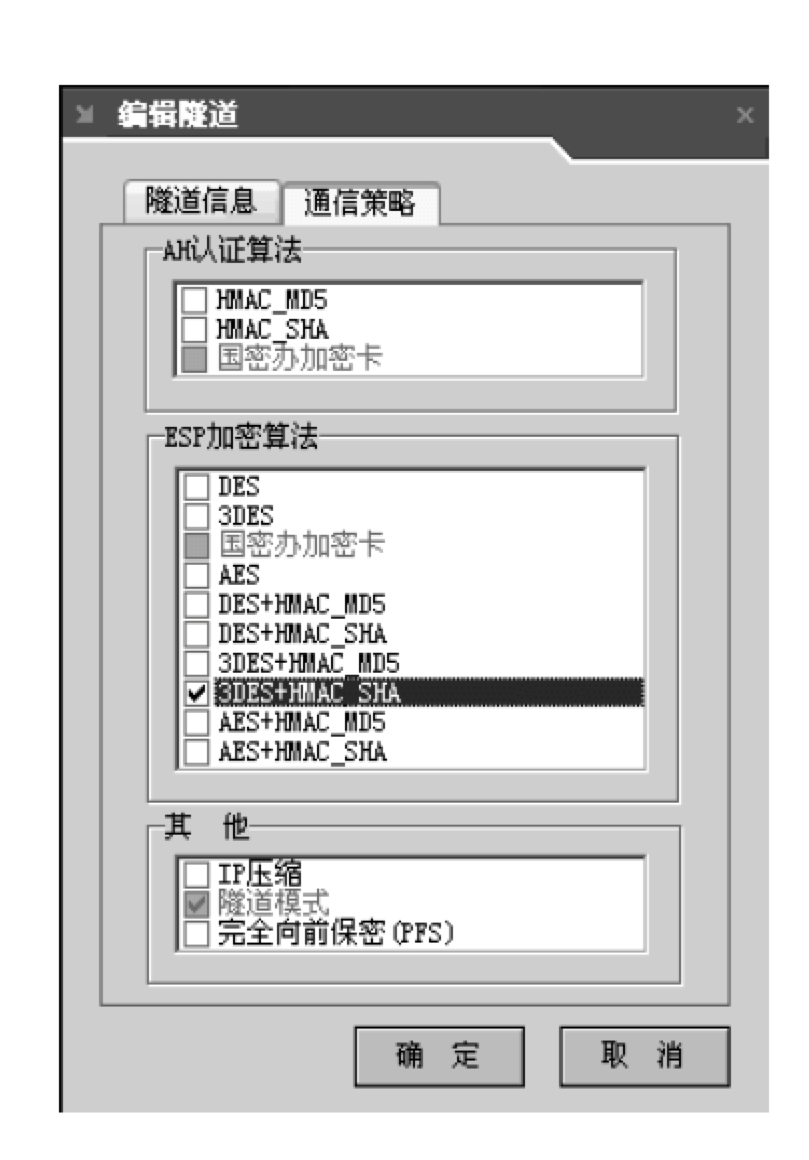



图 7-21　配置隧道通信策略

| 对方设备名称 | 本地设备身份 | 认证方式 | 隧道数量 | 隧道类型 |
|---|---|---|---|---|
| VPNB | 客户端 | 预共享密钥 | 1 | GUI |

添加隧道　删除隧道　编辑隧道　启动隧道　暂停隧道

| 隧道名称 | 对方设备名称 | 本地设备接口 | 对方设备地址 | 本地子网 | 对方子网 |
|---|---|---|---|---|---|
| To_VPNB | VPNB | eth1 | 201.1.1.1 | 192.168.1.0/255.255.255.0 | 192.168.2.0/255.255.255.0 |

图 7-22　完成隧道的配置

### 13. 配置 VPNB 的 LAN-to-LAN IPSec VPN

在 VPNB 的管理界面中，选择"虚拟专用网"→IPSec VPN→"隧道配置"后进入隧道配置页面，然后单击页面上的"添加设备"按钮配置对端 VPN 网关。

在"对方设备名称"文本框中输入对方 VPN 网关的名称，这里我们输入 VPNA；在"本地设备接口"下拉列表中选择在哪个接口上建立 IPSec 隧道，这里我们选择 WAN 接口 eht1；在"本地设备身份"区域中我们选择"作为客户端"单选按钮，并配置"对方设备地址"为 VPNA WAN 接口的地址 200.1.1.3；在"认证方式"区域中我们选择"预共享密钥"单选按钮，并将"密钥"设置为 1234567，密钥在 VPNA 和 VPNB 必须匹配，单击"确定"按钮完成配置，如图 7-23 所示。

完成对端设备的配置后，单击页面上的"添加隧道"按钮配置访问 VPNA 的 IPSec 隧道。

在"隧道信息"选项卡中，"隧道名称"使我们可以为该隧道指定任意的名称，这里我们

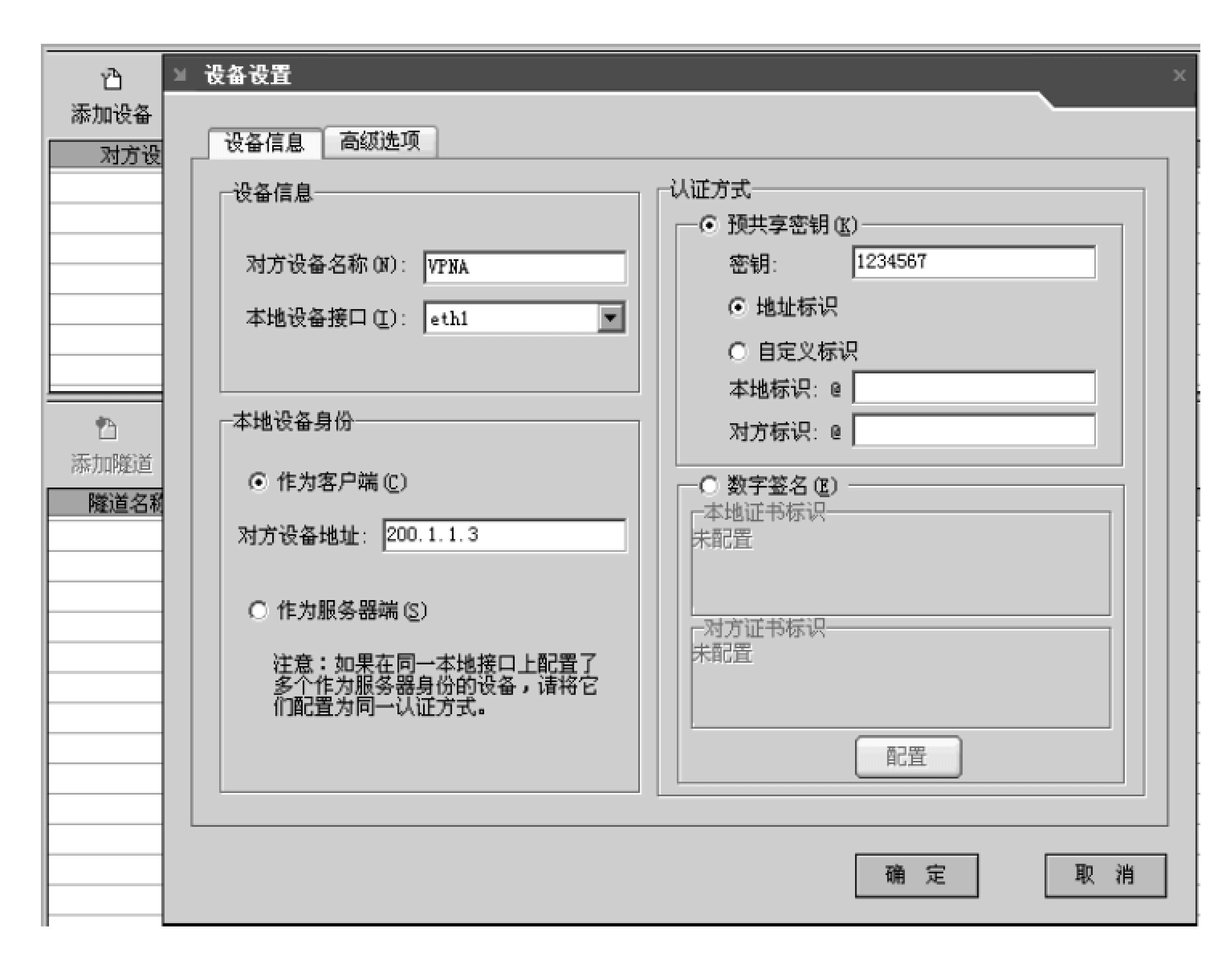



图 7-23　配置虚拟专用网

使用 To_VPNA；在“对方设备名称”下拉列表中选择刚刚创建的对端设备 VPNA；在“本地子网”区域中输入分支办事处网络的子网信息 192.168.2.0/24；在“对方子网”区域中输入总部网络的子网信息 192.168.1.0/24，如图 7-24 所示。

在“通信策略”选项卡中，对于 VPNA 的设备连接默认使用 IPSec 隧道模式。IPSec 默认使用 ESP 协议，加密算法为 3DES，哈希函数使用 SHA。这里也可以指定多个套件，双方会在多个中协商出一个匹配的套件来建立隧道，单击“确定”按钮完成隧道的配置，如图 7-25 所示。

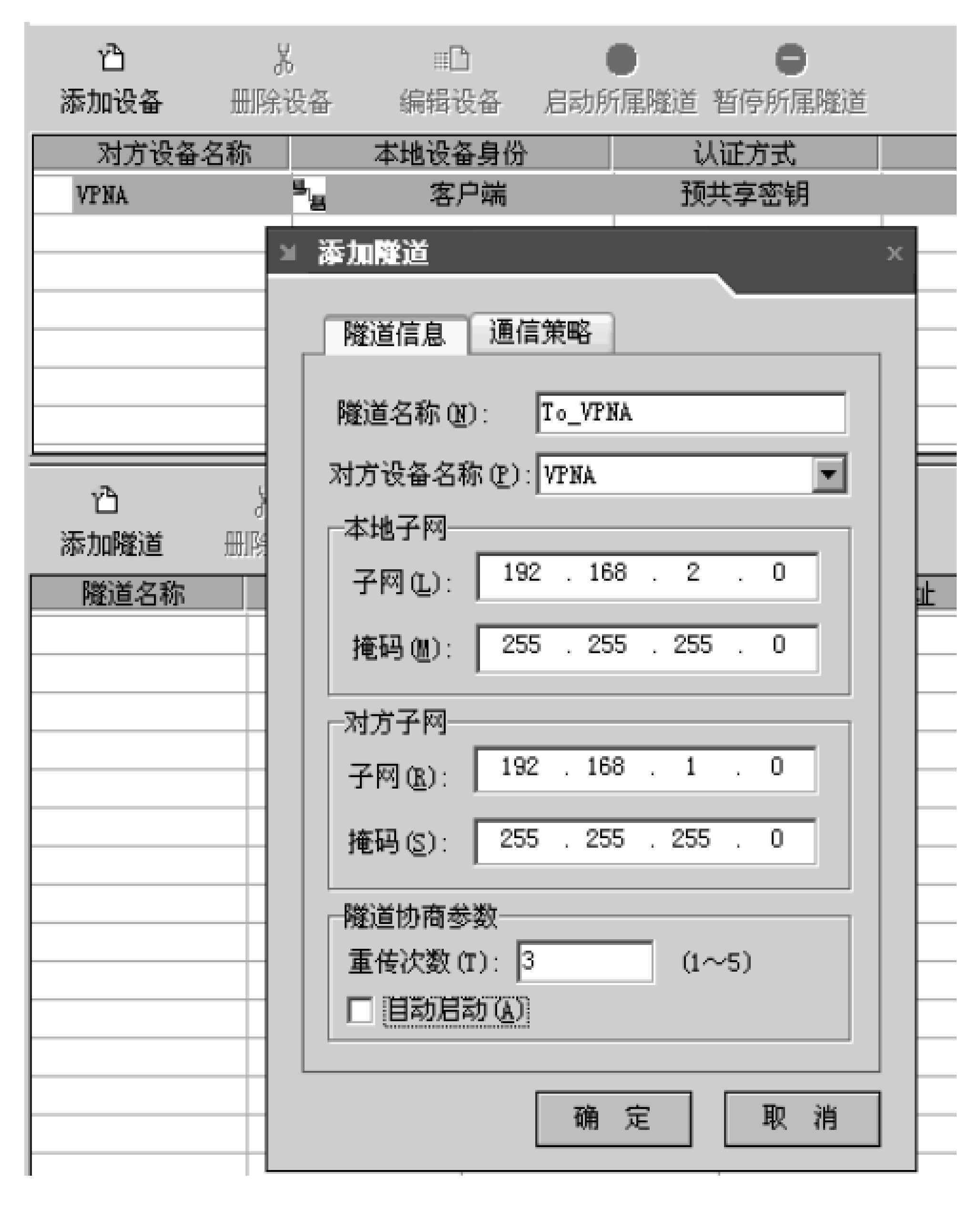



图 7-24　配置隧道信息




图 7-25　配置隧道通信策略

完成后的隧道配置如图 7-26 所示。

| 对方设备名称 | 本地设备身份 | 认证方式 | 隧道数量 | 隧道类型 |
|---|---|---|---|---|
| VPNA | 客户端 | 预共享密钥 | 1 | GUI |

添加隧道　删除隧道　编辑隧道　启动隧道　暂停隧道

| 隧道名称 | 对方设备名称 | 本地设备接口 | 对方设备地址 | 本地子网 | 对方子网 |
|---|---|---|---|---|---|
| To_VPNA | VPNA | eth1 | 200.1.1.3 | 192.168.2.0/255.255.255.0 | 192.168.1.0/255.255.255.0 |

图 7-26　完成隧道配置

### 14. 验证 LAN-to-LAN IPSec VPN

由于 PC1 的默认网关为防火墙 LAN 接口的地址 192.168.1.1，所以为了使发往分支办事处网络的数据被发送到 VPNA 上，在 PC1 上添加一条到达分支办事处网络 192.168.2.0/24 的路由，默认网关为 VPNA 的 LAN 接口地址 192.168.1.2，如图 7-27 所示。

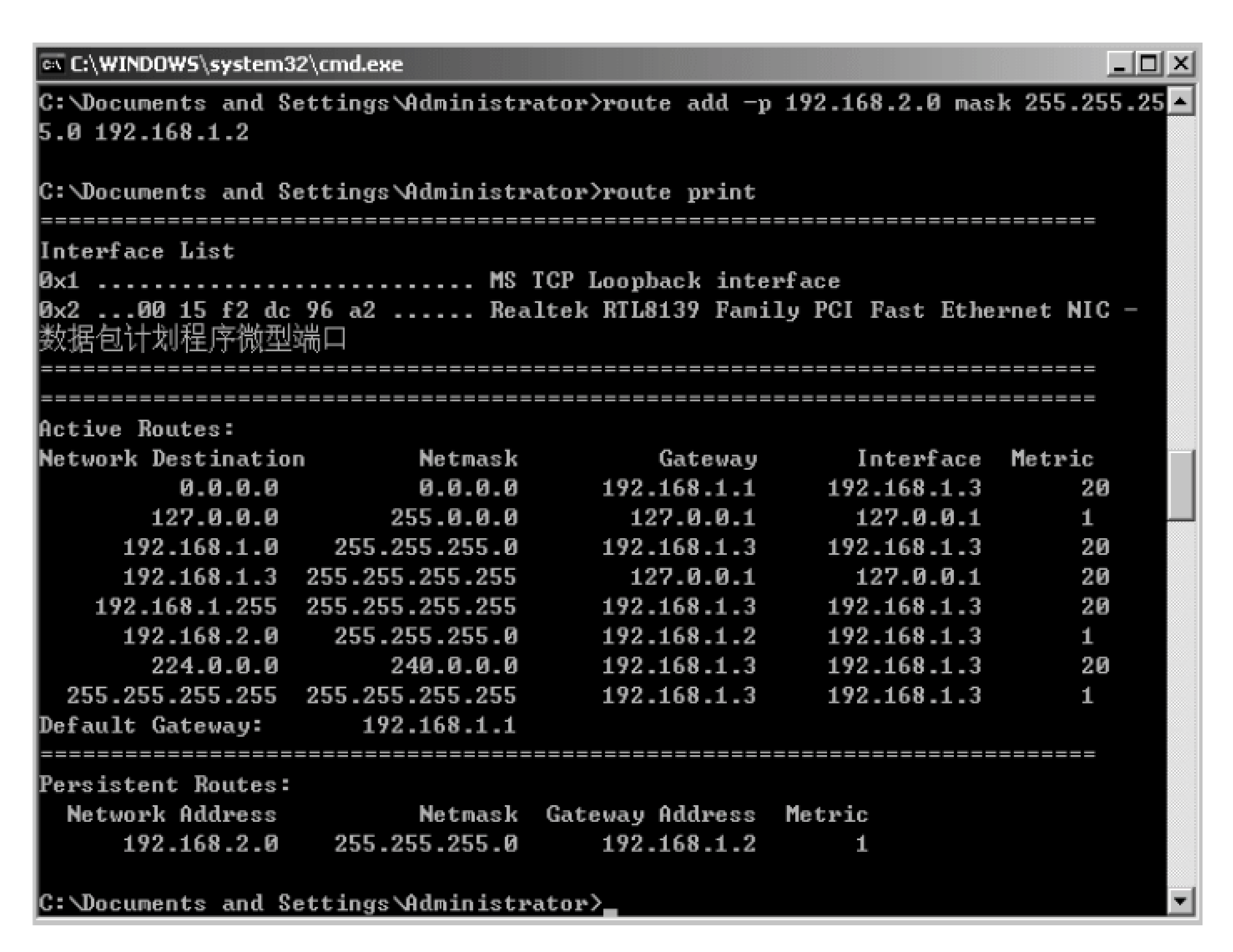



图 7-27　验证隧道配置

在 PC1 上 ping PC2 的地址，可以 ping 通，说明数据是通过总部网络与分支办事处网络的 IPSec 隧道传输，如图 7-28 所示。

在 VPNA 的管理界面中，选择“虚拟专用网”→IPSec VPN→“隧道协商状态”来查看 IPSec 隧道的状态，可以看到 VPNA 和 VPNB 之间的 LAN-to-LAN IPSec 隧道已经协商成功（第二阶段协商成功），如图 7-29 所示。

同样，在 VPNA 的管理界面中，选择“虚拟专用网”→IPSec VPN→“隧道协商状态”来查看 IPSec 隧道的状态，可以看到 VPNA 和 VPNB 之间的 LAN-to-LAN IPSec 隧道已经协商成功（第二阶段协商成功），如图 7-30 所示。

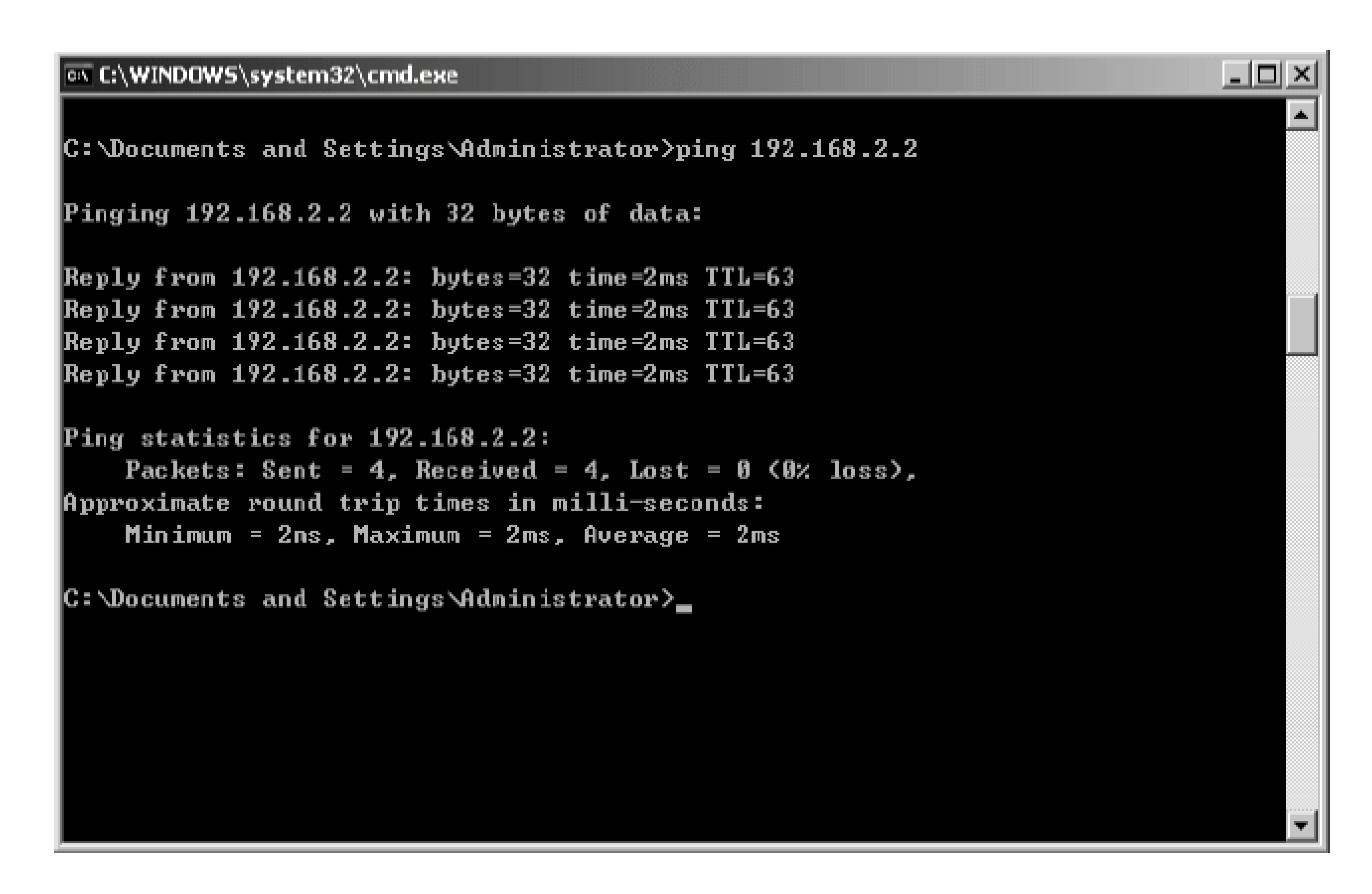



图 7-28　验证配置

隧道协商状态　　隧道状态总数：1条

对方设备名称

| 序号 | 隧道名称 | 隧道状态 | 本地IP | 对方IP | 本地子网 | 对方子网 |
|---|---|---|---|---|---|---|
| 对方设备名称 : VPNB | | | | | | |
| 1 | To_VPNB | 第二阶段协商成功 | 200.1.1.3 | 201.1.1.1 | 192.168.1.0/24 | 192.168.2.0/24 |

图 7-29　查看隧道协商状态

隧道协商状态　　隧道状态总数：1条

对方设备名称

| 序号 | 隧道名称 | 隧道状态 | 本地IP | 对方IP | 本地子网 | 对方子网 |
|---|---|---|---|---|---|---|
| 对方设备名称 : VPNA | | | | | | |
| 1 | To_VPNA | 第二阶段协商成功 | 201.1.1.1 | 200.1.1.3 | 192.168.2.0/24 | 192.168.1.0/24 |

图 7-30　查看 IPSec 隧道的状态

### 15. 配置 VPNA 的 Remote-Access IPSec VPN

在 VPNA 的管理界面中，选择“虚拟专用网”→IPSec VPN→“远程用户管理”后进入远程用户页面，然后单击页面上的“允许访问子网”图标，配置远程用户可以访问总部网络中的子网信息。然后单击“添加”按钮添加允许的子网信息，我们输入总部网络的地址 192.168.1.0 255.255.255.0，单击“确定”按钮完成添加，如图 7-31 所示。




图 7-31　添加允许的子网信息

单击页面上的“本地用户数据库”图标，添加远程用户信息，用户名和密码都为 rauser，然后单击“数据库生效”按钮使添加的用户立即生效，如图 7-32 所示。




图 7-32　添加远程用户信息

单击“远程用户管理”页面上的“虚 IP 地址池”图标，配置分配给远程 IPSec 接入用户的地址信息，这里我们分配给远程用户的子网地址为 192.168.3.0/24。添加完成后，将页面上“对虚 IP 分配表之外的用户不自动分配虚 IP”的复选框取消勾选，因为此案例我们不需要为特定用户指定特定的 IP 地址，如图 7-33 所示。




图 7-33　分配给远程用户的子网地址

## 16. 配置 PC3(IPSec Client)

在 PC3 上安装并启动安全远程接入系统 SRA 软件。新建一个访问总部 VPNA 的

远程连接，网关地址为 VPNA WAN 接口的地址 200.1.1.3，认证方式使用“网关本地认证”，单击“确定”完成创建，如图 7-34 所示。




图 7-34　启动安全远程接入软件

## 17. 验证 Remote-Access IPSec VPN

在安全远程接入系统 SRA 中右键单击刚刚创建的连接，在弹出的菜单中选择“启动连接”命令，系统提示输入用户名和密码，我们使用之前在 VPNA 上创建的本地用户名 rauser，密码为 rauser，单击“连接”按钮，如图 7-35 所示。




图 7-35　启动连接

登录成功后，双击 Windows 右下角的 SRA 图标查看远程 IPSec 隧道的详细信息，可以看到，PC3 可以访问总部网络 192.168.1.0/24，并且获得的私有地址为 192.168.1.3，如图 7-36 所示。




图 7-36　查看远程 IPSec 隧道的详细信息

在 VPNA 的管理界面中，选择“虚拟专用网”→IPSec VPN→“隧道协商状态”来查看 IPSec 隧道的状态，可以看到 PC3 与 VPNA 之间的 Remote-Access IPSec 隧道已经协商成功(第二阶段协商成功)，如图 7-37 所示。

隧道协商状态　　隧道状态总数：2条

对方设备名称

| 序号 | 隧道名称 | 隧道状态 | 本地IP | 对方IP | 本地子网 | 对方子网 |
|---|---|---|---|---|---|---|
| 对方设备名称 : ROCAS_eth1_0105 | | | | | | |
| 1 | ROCAS_eth1_0105_d | 第二阶段协商成功 | 200.1.1.3 | 201.1.1.10 | 192.168.1.0/24 | 192.168.3.1/32 |

图 7-37　查看 IPSec 隧道的状态

在总部的 PC1 上再添加一条到达远程客户端子网 192.168.3.0/24 的路由，网关为 VPNA 的 LAN 接口地址 192.168.1.2，如图 7-38 所示。

在 PC3 上 ping PC1 的地址，可以 ping 通，说明 PC3(IPSec Client)可以通过与 VPNA 的 Remote-Access IPSec 隧道访问总部内部网络，如图 7-39 所示。

### 18. 配置交换机端口镜像

为了使防火墙背后的 IDS 能够侦听到内部网络中的数据流，需要在内部网络的交换机上配置端口镜像，使得将通过交换机的流量镜像到 IDS 监控端口：

```
Switch# configure terminal
Switch(config)# monitor session 1 source interface FastEthernet 0/10 both
Switch(config)# monitor session 1 source interface FastEthernet 0/9 both
Switch(config)# monitor session 1 source interface FastEthernet 0/2 both
Switch(config)# monitor session 1 source interface FastEthernet 0/1 both
Switch(config)# monitor session 1 destination interface FastEthernet 0/20
!配置 SPAN，源端口为 F0/1、F0/2、F0/9、F0/10，目的端口为连接 IDS Sensor 监控端口的 F0/20
```

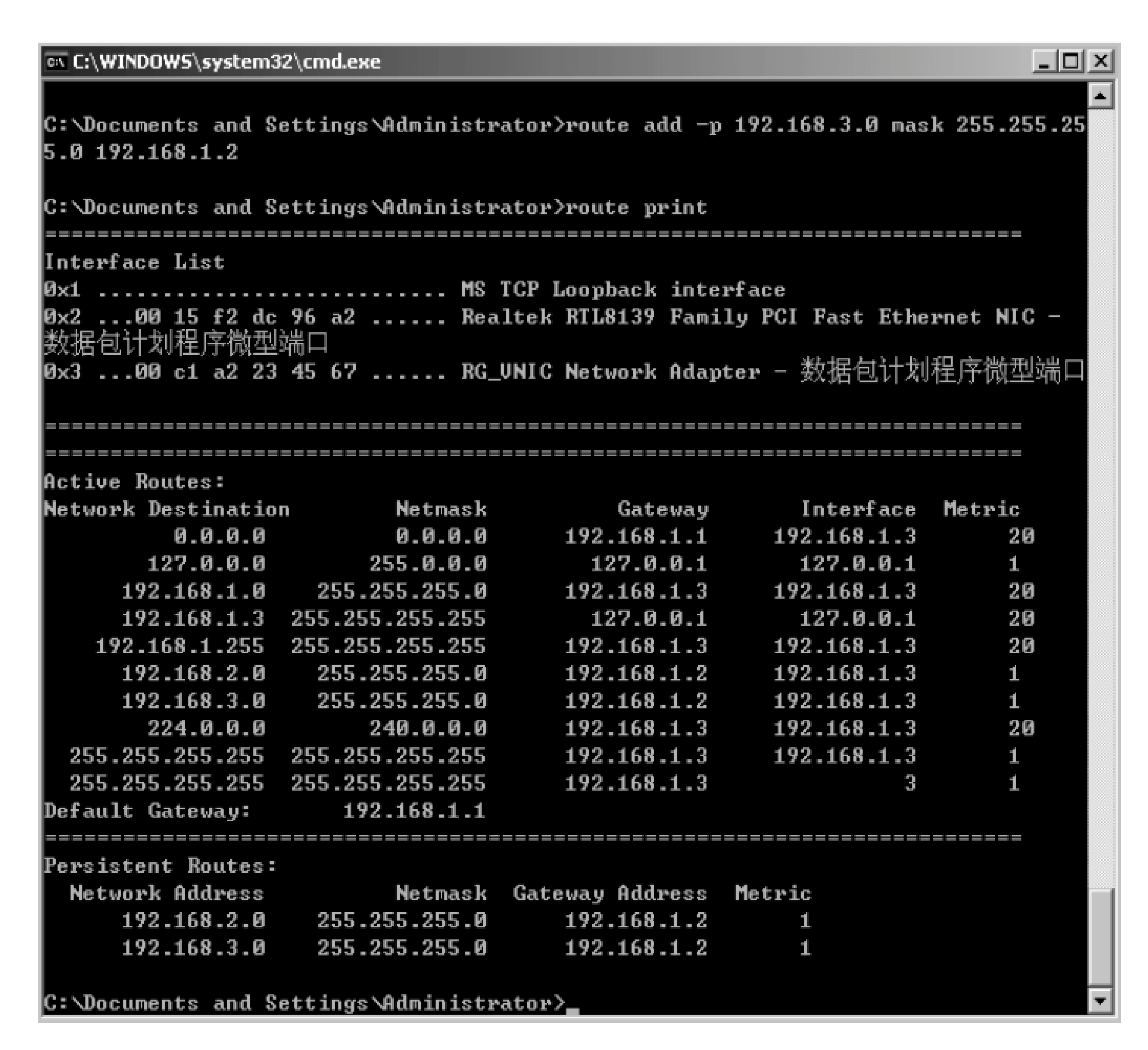



图 7-38　添加一条到达远程客户端子网的路由

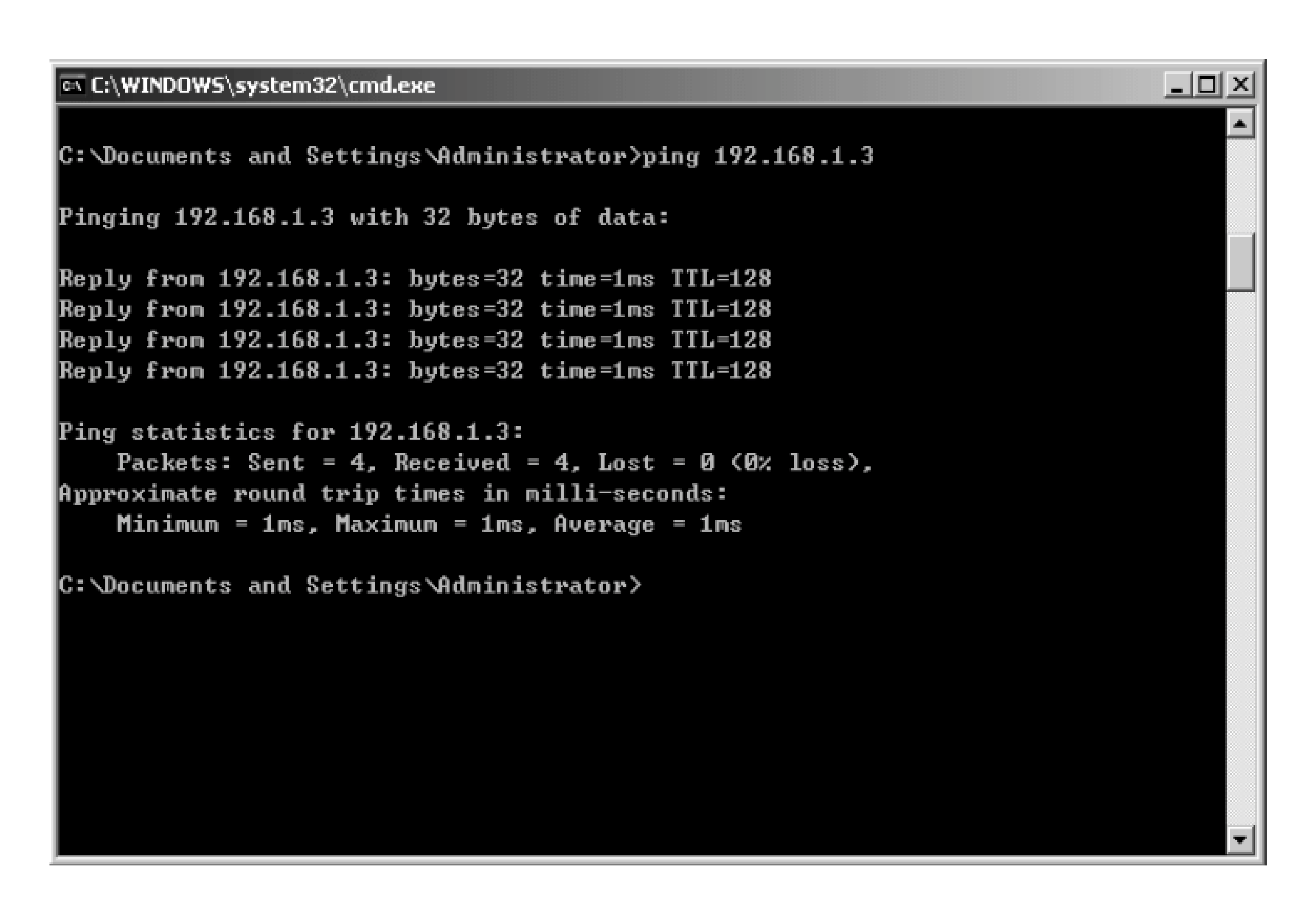



图 7-39　访问总部内部网络

### 19. 配置 IDS Sensor 地址及登录 IDS 控制台

连接到 IDS Sensor 的串口，输入管理员密码后进入到管理菜单，选择 Configure networking，如图 7-40 所示。

配置管理接口的地址为 192.168.4.1，掩码为 255.255.255.0，RG-IDS Server 即事件收集器的地址为 192.168.4.2，保存配置后 IDS Sensor 将重新启动，如图 7-41 所示。

```
+------------------------------------------------------------------------------+
|                              Management Menu                                 |
| RG-IDS Sensor 100                                              Version 7.1.1 |
|                                                                              |
+------------------------------------------------------------------------------+
|                                                                              |
|     Return to status monitor                                                 |
|                                                                              |
|     Access administration                                                    |
|     Set date and time                                                        |
|     Configure networking                                                     |
|     Set interface media and duplex                                           |
|     Network information                                                      |
|     Disable serial console                                                   |
|     Load configuration from floppy                                           |
|     Save configuration to floppy                                             |
|                                                                              |
|     Restart RG-IDS Sensor                                                    |
|     Halt RG-IDS Sensor                                                       |
|     Purge all data                                                           |
|     Uninstall RG-IDS Sensor                                                  |
|                                                                              |
|                                                                              |
+------------------------------------------------------------------ F1: Help -+
```

图 7-40　连接到 IDS Sensor 的串口




图 7-41　配置管理接口的地址

在 PC5 上预先安装 RG-IDS 事件收集器和 RG-IDS 控制台，地址配置为 192.168.4.2/24，然后启动相应的服务后，使用默认的用户名 Admin，密码 Admin，登录 IDS 控制台，由于事件收集器安装在与控制台同一台 PC(PC5)上，所以地址为 127.0.0.1，如图 7-42 所示。




图 7-42　安装 RG-IDS 事件收集器和控制台

登录后，创建一个用户，用户名为 idsuser，密码为 idsuser，并赋予其所有的权限，如图 7-43 所示。



图 7-43　创建一个用户

使用用户 idsuser 重新登录 IDS 控制台，并添加传感器组件，如图 7-44 所示。



图 7-44　添加传感器组件

## 20. 配置 IDS 策略

在 IDS 控制台界面中，单击“策略”按钮，然后右键单击名为 Engine_Inside_FireWall 的策略，在弹出的菜单中选择“编辑锁定”命令，如图 7-45 所示。

再次右键单击名为 Engine_Inside_FireWall 的策略，在弹出的菜单中选择“派生策略” 命令，如图 7-46 所示。

输入策略的名称，这里我们使用 IDS_Sensor，如图 7-47 所示。

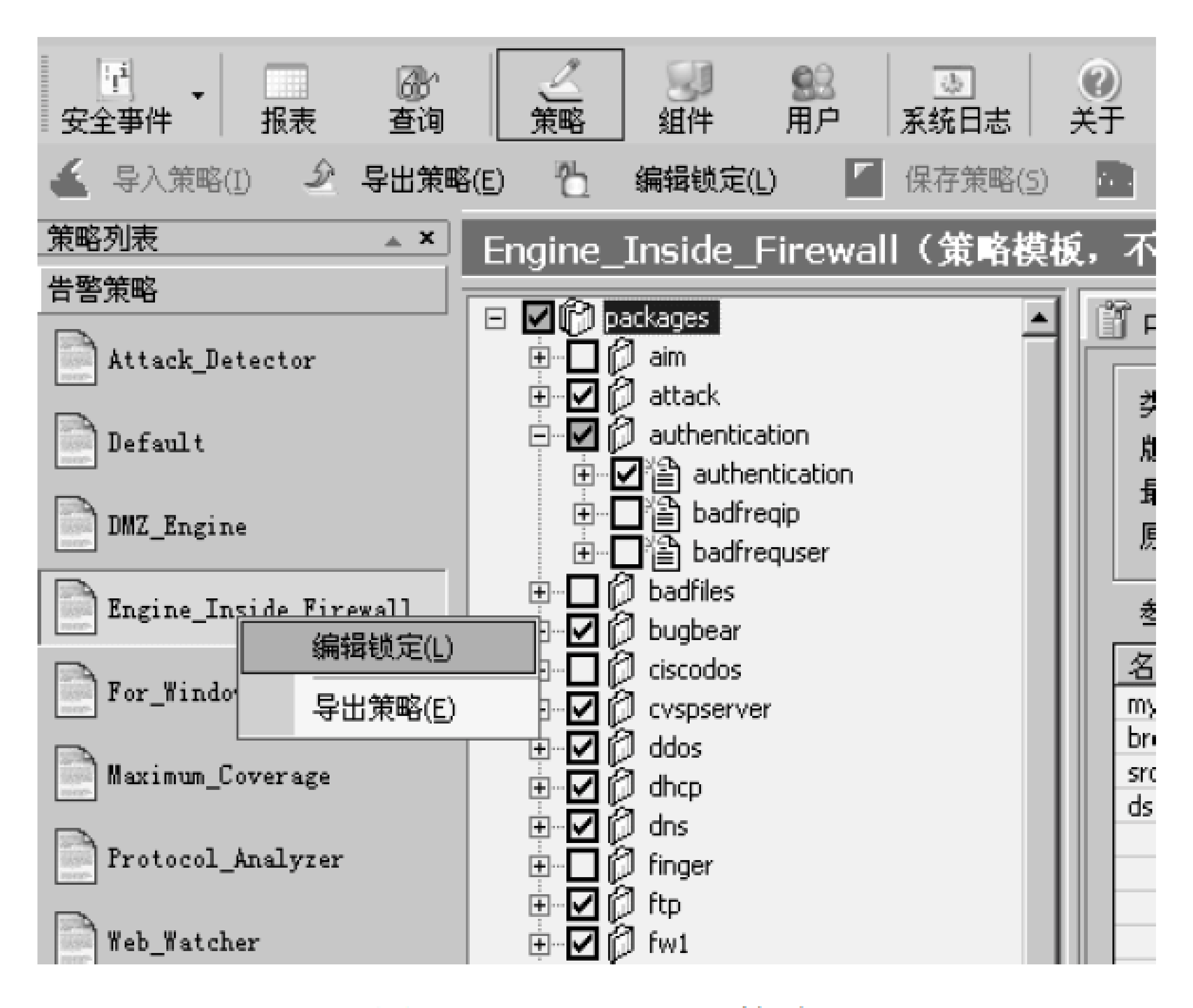



图 7-45　配置 IDS 策略

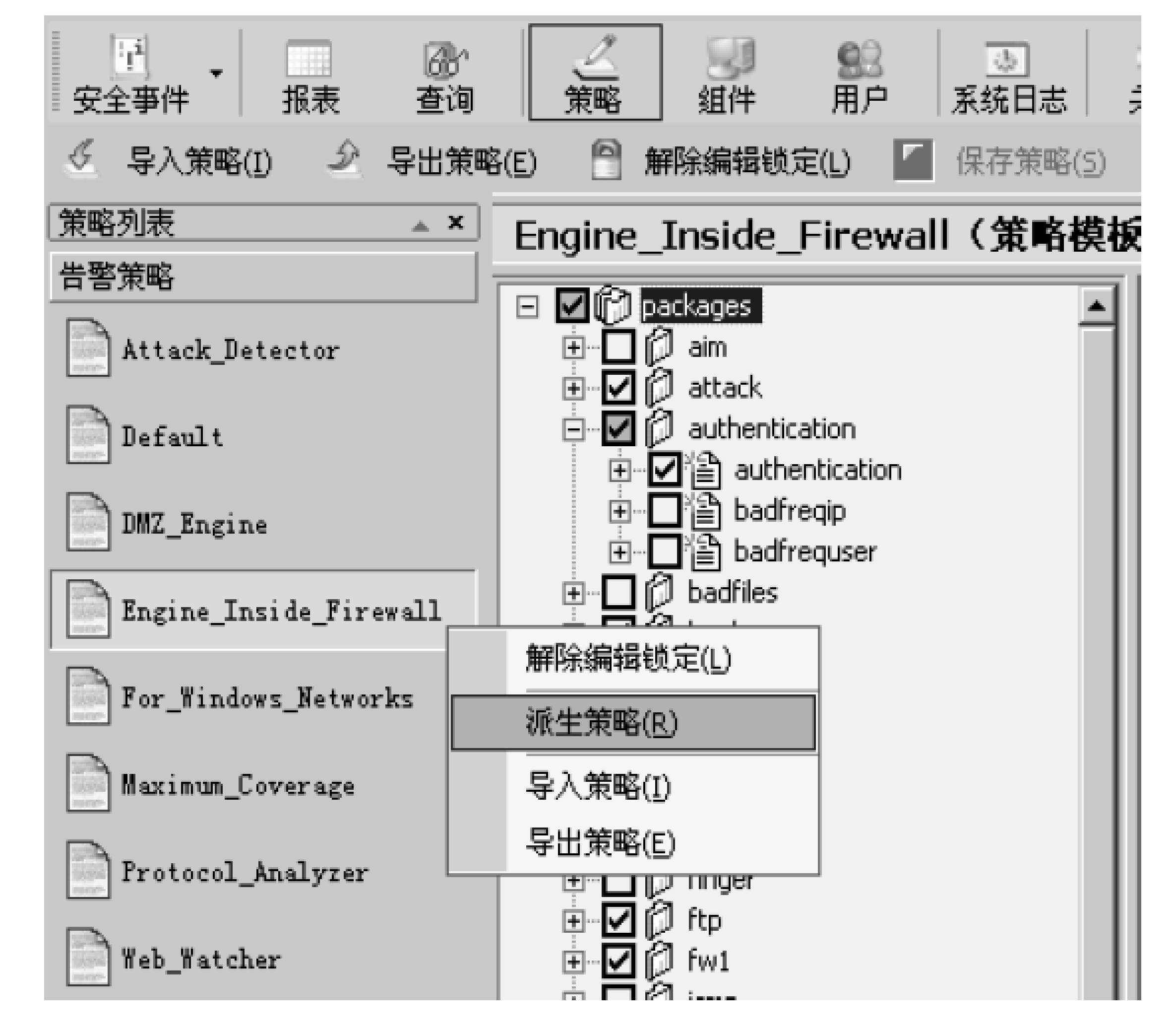








图 7-46　派生策略　　　　图 7-47　输入策略的名称

对派生的策略进行编辑，我们启用 tcp 的所有签名，然后单击页面上的“保存策略”按钮，如图 7-48 所示。

单击界面上的“组件”按钮，然后右键单击 IDS Sensor 组件，在弹出的菜单中选择“应用策略”命令，如图 7-49 所示。

选择刚刚创建的策略 IDS_Sensor，然后单击“应用”按钮，如图 7-50 所示。

应用策略后，界面会显示正在将策略发送给 IDS Sensor，如图 7-51 所示。

## 21. 实施扫描攻击

PC4 的地址配置为 201.1.1.44/24，使用端口扫描工具对 FTP 服务器 200.1.1.100 进行端口扫描，可以看到扫描工具检测到 FTP 服务器上正在开启着多种服务，包括 FTP

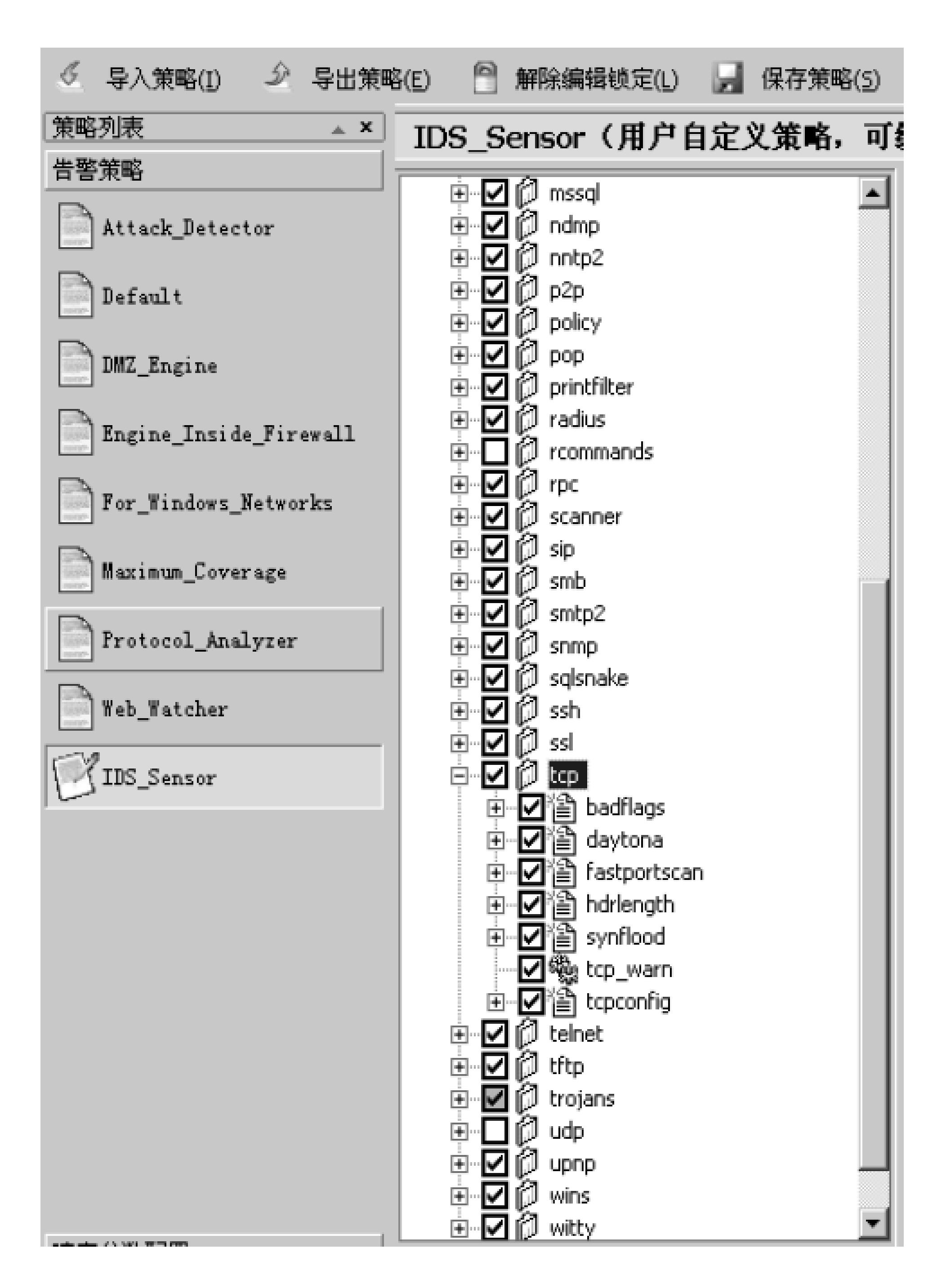



图 7-48 对派生的策略进行编辑




图 7-49 应用策略




图 7-50 应用创建的策略




图 7-51 应用创建的策略

服务,如图 7-52 所示。

## 22 查看 IDS Sensor 安全事件

在 IDS 控制台上查看警报。单击控制台页面中的“安全事件”按钮,可以看到 IDS Sensor 发出“tcp:fastportscan”TCP 快速端口扫描的警告,并且此次威胁来自于 201.1.1.44,即 PC4 的地址,如图 7-53 所示。

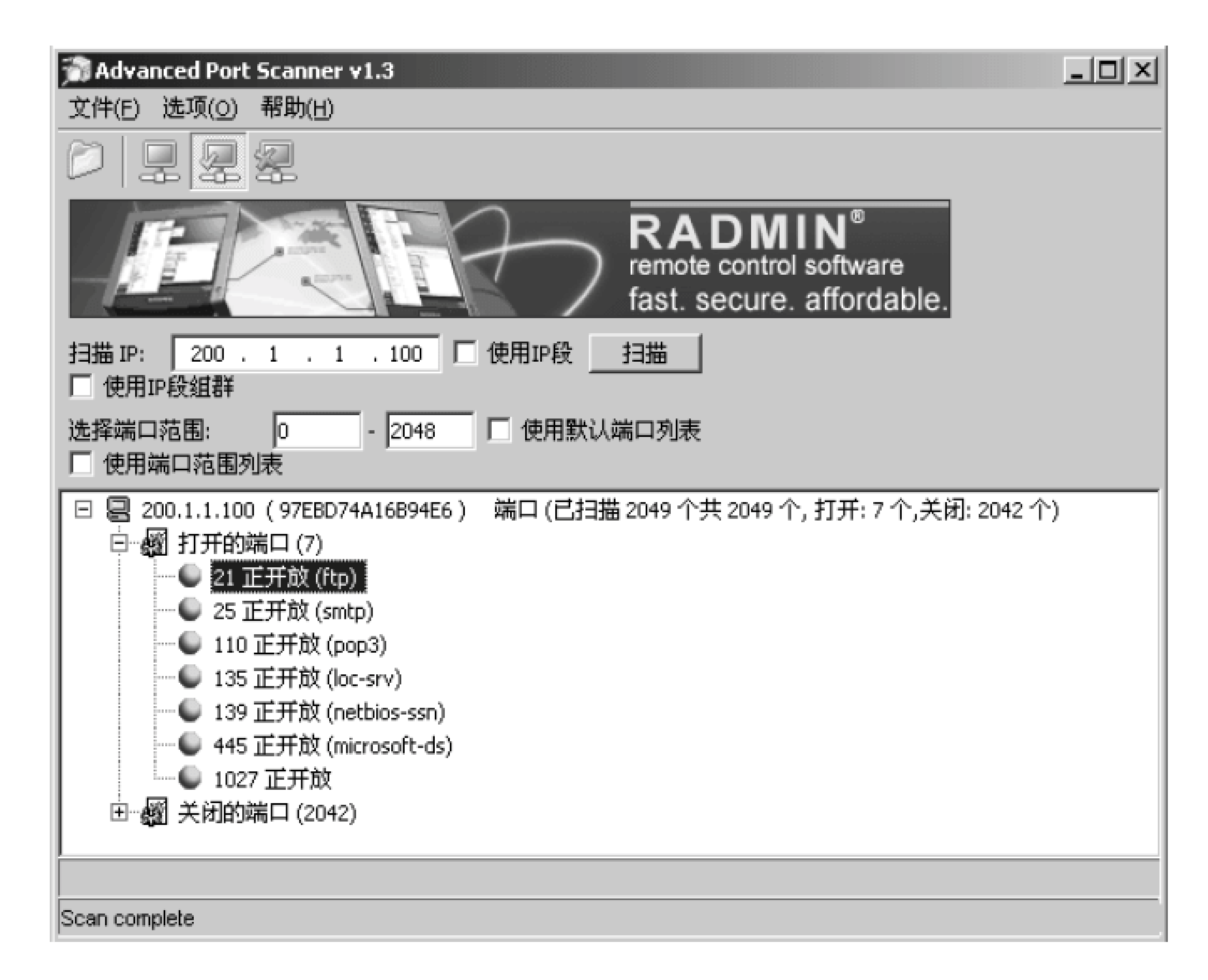



图 7-52　实施扫描攻击

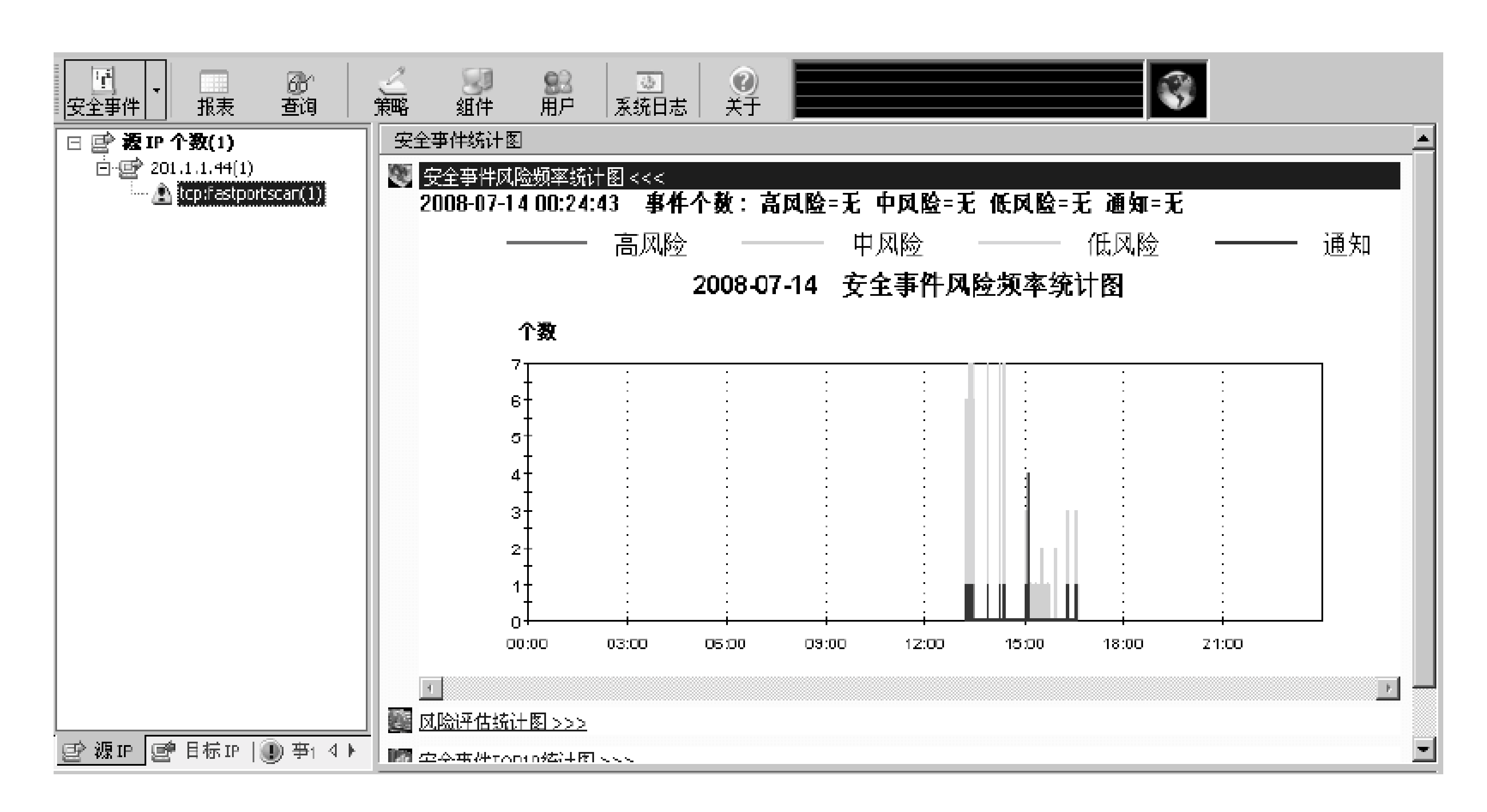



图 7-53　查看 IDS Sensor 告警

## 23. 配置防火墙的抗攻击功能

在防火墙的 Web 界面中，选择“安全策略”→“抗攻击”后进入抗攻击配置页面，对于 WAN 接口单击末尾的操作图标后，勾选“启用抗攻击”复选框，并且选择一个或多个需要启用的抗攻击功能。这里我们将抗 TCP 端口扫描默认的 10 毫秒修改为 1000 毫秒，即如果每秒有访问同一个 IP 的 10 个不同端口的 TCP 包，则认为是 TCP 端口扫描攻击，并且防火墙将阻断源地址并丢弃扫描报文，如图 7-54 所示。

## 24. 实施扫描攻击

再次在 PC4(Attacker)上使用端口扫描工具对 FTP 服务器 200.1.1.100 进行端口扫描，可以看到扫描工具这次无法检测到 FTP 服务器上正在开放的服务，因为扫描报文已经被防火墙阻断，如图 7-55 所示。



图 7-54　配置防火墙的抗攻击功能

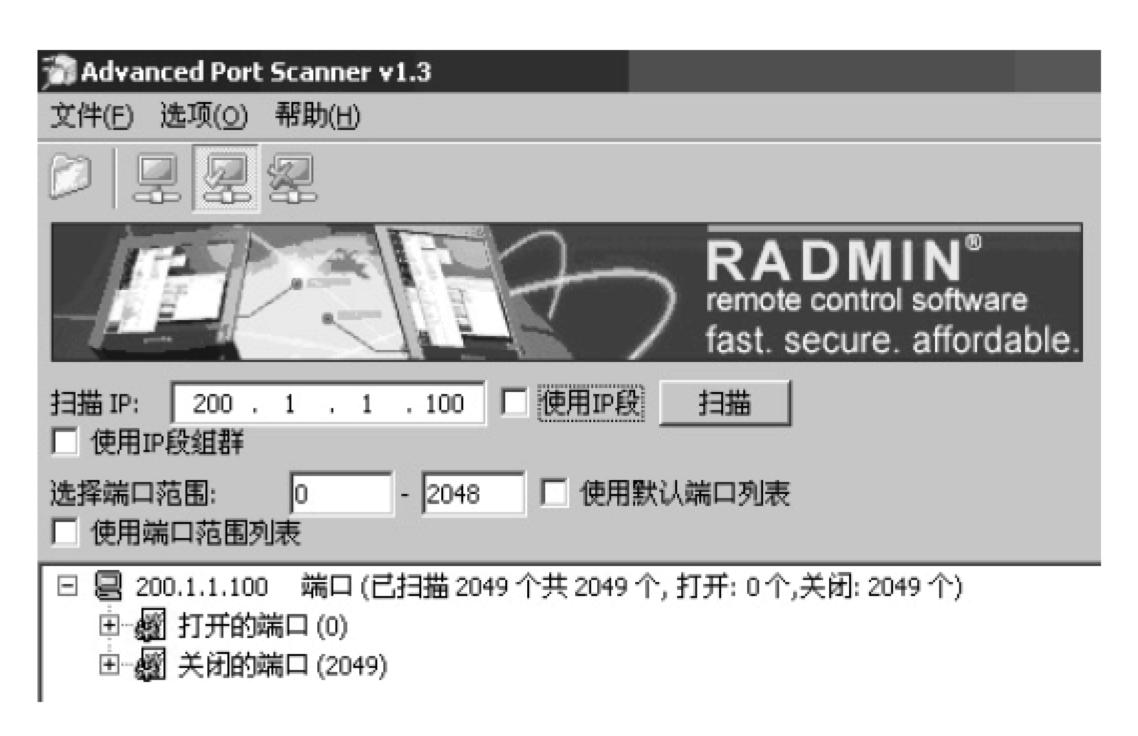


图 7-55　实施扫描攻击

由于防火墙阻断了扫描攻击，所以 IDS Sensor 也没有产生报警，如图 7-56 所示。

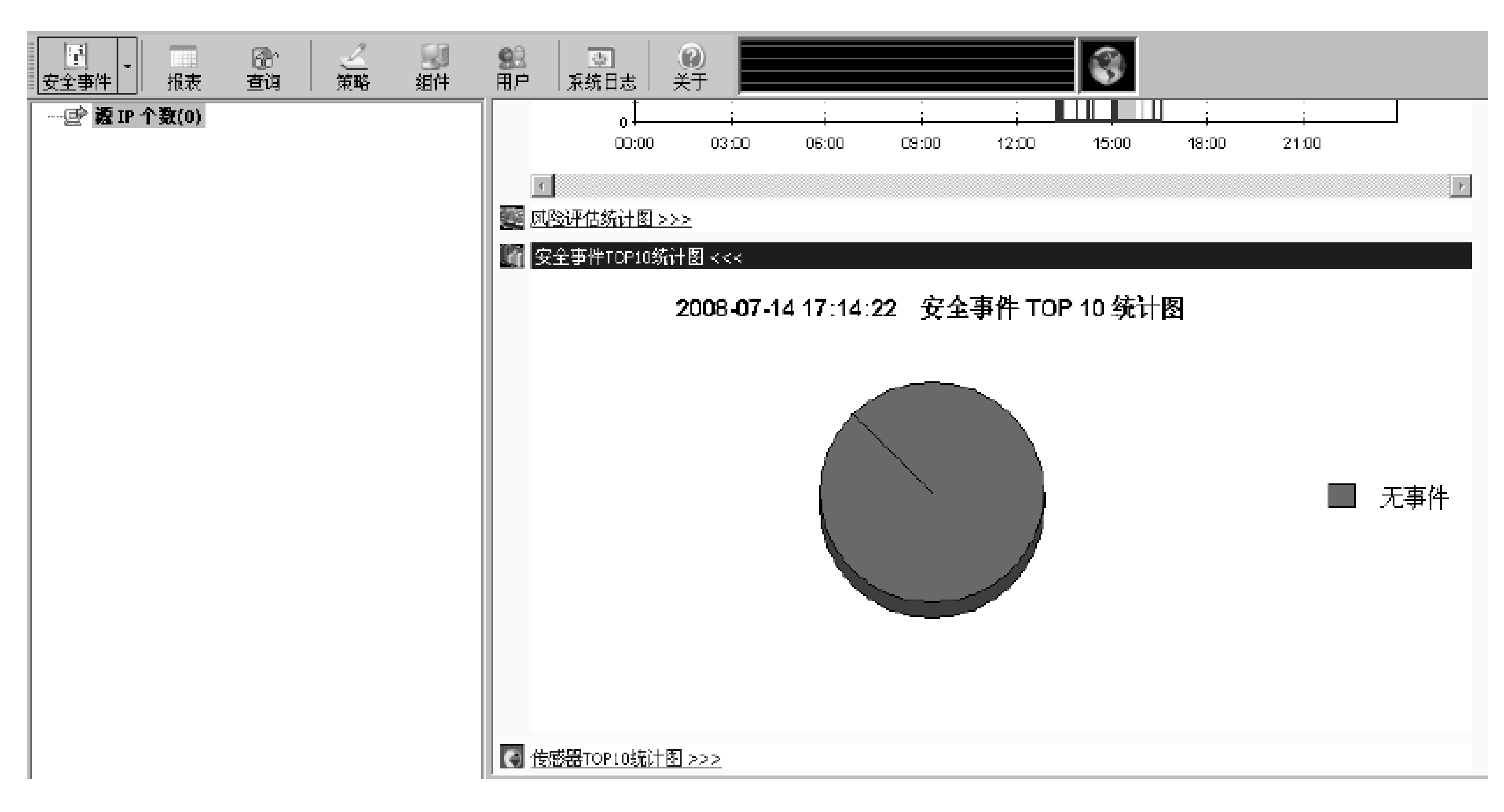


图 7-56　防火墙阻断了扫描攻击

### 25. 配置 RFC 1918 过滤

在运营商的路由器上使用扩展访问控制列表过滤掉源地址为私有地址(RFC 1918)的报文。

```
Router# configure terminal
Router(config)# ip access-list extended deny_rfc1918
Router(config-ext-nacl)# deny ip 192.168.0.0 0.0.255.255 any
Router(config-ext-nacl)# deny ip 172.16.0.0 0.15.255.255 any
Router(config-ext-nacl)# deny ip 10.0.0.0 0.255.255.255 any
Router(config-ext-nacl)# permit ip any any
Router(config-ext-nacl)# exit
Router(config)# interface FastEthernet 0/0
Router(config-if)# ip access-group deny_rfc1918 out
Router(config-if)# end
Router#
```

## 【注意事项】

- 在整个项目实施过程中,建议使用一台专用的 PC 对各个设备进行配置。
- 不要在路由器上配置访问总部网络和分支办事处网络私有子网的路由,因为 Internet 中的路由器是没有访问私有地址的路由条目的。
- 如果要通过 LAN-to-LAN IPSec 隧道和 Remote-Access IPSec 隧道访问 FTP 服务器,需要在 FTP 服务器上添加访问分支办事处网络 192.168.2.0/24 和远程接入用户子网 192.168.3.0/24 的路由。
- 在 Windows 中使用 route add 命令添加静态路由时,使用-p 参数可以添加一条永久路由。
- 在 PC 安装 SRA 后,可能需要重新启动 PC。
- SRA 软件可能会与某些软件产生冲突而不能正常工作。
- 在安装 IDS 组件时,请先安装事件收集器,然后安装控制台。本实验只安装了 IDS 的两个必需的组件,即事件收集器和控制台,如果需要报表功能,请安装数据库和报表查询工具。
- 当使用端口扫描工具进行扫描时,请注意调整扫描的频率,如果扫描的频率过低,防火墙和 IDS 可能将认为是正常的数据流,从而不会阻断和告警。

# 参 考 文 献

［1］ 张敏波．网络安全实战详解．北京：电子工业出版社，2008．
［2］ 姚羽．网络安全与管理项目实验指导书．北京：电子工业出版社，2007．
［3］ 楚狂．网络安全与防火墙技术．重庆：重庆大学出版社，2005．
［4］ Wes Noonan Ido Dubrawsky．防火墙基础．北京：人民邮电出版社，2007．
［5］ Keith E Strassberg．防火墙技术大全．北京：机械工业出版社，2008．
［6］ 马春光．防火墙、入侵检测与VPN．北京：北京邮电大学出版社，2008．
［7］ Rebdcca Gurley Bace．入侵检测．北京：人民邮电出版社，2007．

# 读者意见反馈

亲爱的读者：

感谢您一直以来对清华版计算机教材的支持和爱护。为了今后为您提供更优秀的教材，请您抽出宝贵的时间来填写下面的意见反馈表，以便我们更好地对本教材做进一步改进。同时如果您在使用本教材的过程中遇到了什么问题，或者有什么好的建议，也请您来信告诉我们。

地址：北京市海淀区双清路学研大厦 A 座 602 室 计算机与信息分社营销室 收

邮编：100084　　电子邮件：jsjjc@tup.tsinghua.edu.cn

电话：010-62770175-4608/4409　　邮购电话：010-62786544

教材名称：网络安全防御技术实践教程

ISBN：978-7-302-20983-6

**个人资料**

姓名：________ 年龄：______ 所在院校/专业：__________

文化程度：________ 通信地址：__________________

联系电话：________ 电子信箱：__________________

**您使用本书是作为：**□指定教材 □选用教材 □辅导教材 □自学教材

**您对本书封面设计的满意度：**

□很满意 □满意 □一般 □不满意　改进建议__________________

**您对本书印刷质量的满意度：**

□很满意 □满意 □一般 □不满意　改进建议__________________

**您对本书的总体满意度：**

从语言质量角度看 □很满意 □满意 □一般 □不满意

从科技含量角度看 □很满意 □满意 □一般 □不满意

**本书最令您满意的是：**

□指导明确 □内容充实 □讲解详尽 □实例丰富

**您认为本书在哪些地方应进行修改？（可附页）**

______________________________________________

______________________________________________

**您希望本书在哪些方面进行改进？（可附页）**

______________________________________________

______________________________________________

# 电子教案支持

敬爱的教师：

为了配合本课程的教学需要，本教材配有配套的电子教案（素材），有需求的教师可以与我们联系，我们将向使用本教材进行教学的教师免费赠送电子教案（素材），希望有助于教学活动的开展。相关信息请拨打电话 010-62776969 或发送电子邮件至 jsjjc@tup.tsinghua.edu.cn 咨询，也可以到清华大学出版社主页（http://www.tup.com.cn 或 http://www.tup.tsinghua.edu.cn）上查询。